CHARACTER SUMS, ALGEBRAIC FUNCTION FIELDS, CURVES WITH MANY RATIONAL POINTS AND GEOMETRIC GOPPA CODES

A THESIS

SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCES
OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

By

Ferruh Özbudak

August, 1997

CHARACTER SUMS, ALGEBRAIC FUNCTION FIELDS, CURVES WITH MANY RATIONAL POINTS AND GEOMETRIC GOPPA CODES

A THESIS

SUBMITTED TO THE DEPARTMENT OF MATHEMATICS

AND THE INSTITUTE OF ENGINEERING AND SCIENCES

OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

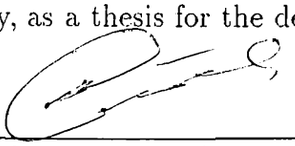
DOCTOR OF PHILOSOPHY

By

Ferruh Özbudak

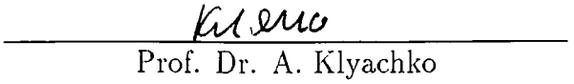
August, 1997

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.



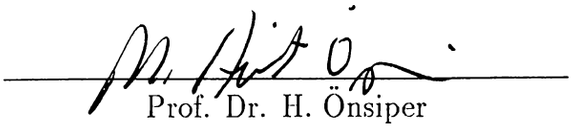
Prof. Dr. S.A. Stepanov(Principal Advisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.



Prof. Dr. A. Klyachko

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.



Prof. Dr. H. Önsiper

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. A. Shumovsky

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.

Asst. Prof. Dr. Yalçın Yıldırım

Approved for the Institute of Engineering and Sciences:

Prof. Dr. Mehmet Baray
Director of Institute of Engineering and Sciences

ABSTRACT

CHARACTER SUMS, ALGEBRAIC FUNCTION FIELDS, CURVES WITH MANY RATIONAL POINTS AND GEOMETRIC GOPPA CODES

Ferruh Özbudak
Ph. D. in Mathematics
Advisor: Prof. Dr. S.A. Stepanov
August, 1997

In this thesis we have found and studied fibre products of hyperelliptic and superelliptic curves with many rational points over finite fields. We have applied Goppa construction to these curves to get "good" linear codes. We have also found a nontrivial connection between configurations of affine lines in the affine plane over finite fields and fibre products of Kummer extensions giving "good" codes over $\mathbb{F}_{q^2}$. Moreover we have calculated an important parameter of a class of towers of algebraic function fields over finite fields, which are studied recently.

Keywords : Algebraic curve, algebraic function field, finite field, Goppa code.

ÖZET

KARAKTER TOPLAMLARI, CEBIRSEL FONKSIYON CISIMLERI, FAZLA RASYONEL NOKTALI EĞRILER VE GEOMETRIK GOPPA KODLARI

Ferruh Özbudak
Matematik Bölümü Doktora
Danışman: Prof. Dr. S.A. Stepanov
Ağustos, 1997

Bu çalışmada üzerinde fazla rasyonel nokta bulunan sonlu cisimler üzerindeki hipereliptik ve supereliptik eğrilerinin fiber çarpımları bulundu ve çalışıldı. Bu eğrilere Goppa metodu uygulanarak "iyi" kodlar bulundu. Sonlu cisimler üzerindeki afine düzleminin içindeki afine doğrularının konfigürasyonlarıyla Kummer genişletmelerinin fiber çarpımları arasında "iyi" kodlar veren ilginç bir bağlantı bulundu. Ayrıca sonlu cisimler üzerindeki son zamanlarda çalışılmış olan bir tür cebirsel fonksiyon cisimlerinin önemli bir parametresi hesaplandı.

Anahtar Kelimeler : Cebirsel eğri, cebirsel fonksiyon cismi, sonlu cisim, Goppa kodları.

ACKNOWLEDGMENTS

I would like to thank my advisor Serguei A. Stepanov for his excellent guidance, his readiness to help me, and his marvelous ideas during my graduate studies at Bilkent University. I would like to thank Henning Stichtenoth for inviting me to Universität Essen, his excellent hospitality, and for fruitful conversations with him. I would also like to thank to Mehpare Bilhan, Alexander Degtyarev, İbrahim Dibağ, Arnaldo Garcia, Metin Gürses, Azer Kerimov, Alexander Klyachko, Mefharet Kocatepe, Uğurhan Muğan, Iossif Ostrovskii, Ruud Pellikaan, Sinan Sertöz, Okan Tekman, Michael Thomas, Fernando Torres, Michael Tsfasman, Yalçın Yıldırım, and all of my teachers and friends at Bilkent University, METU, and Universität Essen for inspiration and their encouragement. Without their support, this thesis would never appear.

I thank to TÜBİTAK for their support of my visit to Universität Essen.

The last but not the least, of course I would like to thank to my family, all of my friends and all of my teachers (of course, there exist a lot of intersections!).

TABLE OF CONTENTS

Chapter 1

Algebraic Curves, Algebraic Function Fields, Linear Codes and Character Sums

The purpose of this chapter is to recall some of the fundamental definitions and relations. For further details see [44], [45], [50], [54], [23], and [24].

1.1 Algebraic Curves and Algebraic Function fields

Let k be an algebraically closed field. A *projective (affine) algebraic curve* X is a projective (affine) algebraic variety of dimension 1. A projective (affine) curve X is called *irreducible* if it cannot be written as $X = X_1 \cup X_2$ where X_1 and X_2 are projective (affine) curves.

A point $P \in X$ is *nonsingular* (or *simple*) if the local ring $\mathfrak{O}_P(X)$ is a discrete valuation ring. Otherwise P is called a *singular* point. There exists only finitely many singular points on a curve. The curve X is called *nonsingular* (or *smooth*) if all points $P \in X$ are nonsingular.

Let X be a projective curve. Then there exists a nonsingular curve X' and a birational morphism $\phi' : X' \to X$. The pair (X', ϕ') is unique in the following sense: If $\phi'' : X'' \to X$ is another birational morphism and X'' is another

nonsingular curve, then there exists a unique isomorphism $\phi : X'' \to X'$ such that $\phi' = \phi'' \circ \phi$. (X', ϕ') or by abuse of language X' is called the *nonsingular model* of X.

$\mathbb{A}^1$ and $\mathbb{P}^1$ are the simplest kinds of affine and projective irreducible smooth curves, lines.

Let $X \subset \mathbb{P}^n$ be an affine or projective variety. Let $f,\ g \in k[x_0, x_1, \ldots, x_n]$ be two forms of the same degree in homogenous coordinates and g is not identically zero on X. Then f/g defines a rational function on X. We say $f/g = f'/g'$ if $fg' - f'g$ is identically zero on X. The set of all rational functions form a field, called the *field of rational functions* on X, denoted by $k(X)$. Note that rational functions are rational morphisms from X to $\mathbb{P}^1$. Recall that if there exists a birational morphism between the curves X and Y, then $k(X) = k(Y)$. If the rational function is a morphism from X to $\mathbb{A}^1 \subsetneq \mathbb{P}^1$, then it is called a *regular function.*

Let X be a smooth irreducible projective curve over k. A *divisor* D on X is a finite formal sum $D = \sum_{P \in X} a_p \cdot P$ where $a_P \in \mathbb{Z}$. The set of all divisors on X forms an abelian group denoted by $Div(X)$. Degree of a divisor $\deg D$ is an additive homomorphism defined by

$$\deg D : Div(X) \to \mathbb{Z}, \quad D = \sum_{P \in X} a_P \cdot P \mapsto \sum_{P \in X} a_P.$$

Let $D \in Div(X)$. Then $L(D) = \{f \in k(X) \mid (f) + D \geq 0\} \cup \{0\}$ is a vector space over k. For any $D \in Div(X)$

$$\dim L(D) - \dim(K - D) = \deg D - g + 1$$

is an important equality, called *Riemann-Roch* theorem. Here g is the *genus* of the curve and K is the *canonical divisor.* Since dimension is nonnegative, $\dim L(D) \geq \deg D - g + 1$. Moreover $\dim(K - D) = 0$ if $K > D$.

An algebraic field extension k'/k is separable if for any $\alpha \in k'$, its minimal polynomial $p_\alpha(x) \in k[x]$ is a separable polynomial. A field k is called *perfect* if all algebraic extensions k'/k are separable. If *char* $k = 0$ or $\mid k \mid < \infty$, then k is perfect.

Now assume that k is a perfect field and $\bar{k}$ is its algebraic closure. Let $X \subset \mathbb{A}^n(k)$ be an affine algebraic curve over k, i.e. $I(X) \in k[x_1, x_2, \ldots, x_n]$. The set $X(k) = X \cap \mathbb{A}^n$ is called the *k-rational points of* X. Equivalently if $Gal(\bar{k}/k)$ is the Galois group of $\bar{k}/k$, then $X(k)$ is the stabilizer of the action

of $Gal(\bar{k}/k)$ on $\mathbb{A}^n(k)$. Similarly $D = \sum_{P \in X} a_P \cdot P$ is a *k-rational divisor of* X if D is stabilized under the action of $Gal(\bar{k}/k)$. Note that the support of a k-rational divisor may have points which are not k-rational.

An *algebraic function field* F/k of one variable over k is an extension field $k \subset F$ such that F is a finite algebraic extension of $k(x)$ for some element $x \in F$ which is transcendental over k. If k is a perfect field, then any algebraic function field F/k corresponds to an affine plane curve $X : g(x,y) = 0$, where x is a separating element for F/k, $F = k(x,y)$ and $g(x,y) \in k[x,y]$ is the irreducible polynomial with $g(x,y) = 0$.

A *valuation ring* of the algebraic function field F/k is a ring $\mathfrak{O} \subset F$ such that $k \subsetneq \mathfrak{O} \subsetneq F$ and if $z \in F$, then $z \in \mathfrak{O}$ or $z^{-1} \in \mathfrak{O}$. A *place* P of the algebraic function field F/k is the maximal ideal of a valuation ring $\mathfrak{O}$ of F/k.

1.2 Linear Codes and Goppa Construction

Let F_q be a finite field with q elements. Let d be the *Hamming distance* on $F_q^n = F_q \times \cdots \times F_q$ defined by

$$d(a,b) = \mid \{i : a_i \neq b_i\} \mid$$

where $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$. An $[n,k,d]_q$linear code C is a k dimensional vector space of F_q^n with $d = \min_{a,b \in C} d(a,b)$, the *minimum distance.* The relative parameters of the linear code $[n,k,d]_q$ are defined as

1. $R = \frac{k}{n}$: rate
2. $\delta = \frac{d}{n}$: relative minimum distance

There exists a bound on d

$$d \leq n - k + 1 \text{ or equivalently } R \leq 1 - \delta + \frac{1}{n}$$

which is called as the *Singleton bound.*

By a "good" code we mean n is large compared to q and the Singleton bound is nearly achieved.

Now we recall the Goppa construction [19] which associates a linear $[n,k,d]_q$ code to a smooth projective curve X of genus g defined over a finite field F_q.

Let $\mathfrak{P} = \{P_1, \ldots, P_n\}$ be a set of F_q-rational points of X and set

$$D_0 = P_1 + \cdots + P_n$$

as the corresponding F_q-rational divisor. Let D be an F_q-rational divisor on X whose support is disjoint from D_0. the linear $[n, k, d]_q$ code C is the image of the linear evaluation map

$$Ev: \ L(D) \to F_q^n, \quad f \mapsto (f(P_1), \ldots, f(P_n)).$$

If $\deg D < n$, then Ev is an embedding and therefore $k = \dim C = \dim L(D)$ by Riemann-Roch theorem

$$k \geq \deg D - g + 1.$$

Moreover $d \geq n - \deg D$. Therefore

$$n + 1 - g \leq k + d \leq n + 1,$$

where g is the "defect" of the Singleton bound.

For $X = \mathbb{P}^1$ Goppa construction gives Reed-Solomon codes which are used in CD-players and Hubble telescope! However $n \leq q$ for Reed-Solomon codes and to construct long codes with "small" Singleton defects are important both in theory and application.

1.3 Some Bounds on Linear Codes

Let F_q be a finite field with q elements and

$$V_q = \{(\delta(C), R(C)) \in [0,1] \times [0,1] \mid C \text{ is a linear code over } F_q\}.$$

Denote by $U_q \subset V_q$ the set of limit points of V_q. Manin [26] proved the existence of a continuous function $\alpha_q : [0,1] \to [0,1]$ such that

$$U_q = \{(\delta, R) \mid 0 \leq \delta \leq \text{ and } 0 \leq R \leq \alpha_q(\delta)\}.$$

We know $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ for $1 - \frac{1}{q} \leq \delta \leq 1$ and α_q is decreasing in $0 \leq \delta \leq 1 - \frac{1}{q}$. However the exact value of $\alpha_q(\delta)$ is unknown. There exists several upper and lower bounds for $\alpha_q(\delta)$. For example let $H_q : [0, 1 - \frac{1}{q}] \to \mathbb{R}$ be the *q-ary entropy function* defined by

$$H_q(0) = 0, \ H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$$

for $0 \leq x \leq 1 - \frac{1}{q}$. then for $0 \leq \delta \leq 1 - \frac{1}{q}$

i) *Bassalygo-Elias bound:* $\alpha_q(\delta) \leq 1 - H_q(\theta - \sqrt{\theta(\theta - \delta)})$ where $\theta = 1 - \frac{1}{q}$ and

ii) *Gilbert-Varshamov bound:* $\alpha_q(\delta) \geq 1 - H_q(\delta)$.

The Gilbert-Varshamov bound is not constructive.

Let

$N_q(g) = \max\{N(F) \mid F$ is an algebraic function field over F_q of genus $g\}$

and

$$A_q = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

Then (see [50] page 208)

$$\alpha_q(\delta) \geq (1 - \frac{1}{A(q)}) - \delta.$$

Ihara [22] and Tsfasman-Vladut-Zink [55] proved that $A(q) \geq q^{1/2} - 1$ for $q = q_1^2$. Consequently this improves Gilbert-Varshamov bound in a certain interval for all $q \geq 49$ if q is a square. However the equations for the sequence of curves could not be written. Recently Garcia-Stichtenoth [12] [13] gave explicit sequences of curves over F_q with the optimal value of A_q for q is a square.

1.4 Character Sums

Let F_q be a finite field with q elements. A group homomorphism χ from the multiplicative group F_q^* to the multiplicative group $\mathbb{C}^*$ is called a *multiplicative character* of F_q.

A group homomorphism ψ from the additive group F_q to the multiplicative group $\mathbb{C}^*$ is called an *additive character* of F_q. Therefore

$$\chi : F_q^* \to \mathbb{C}^* \text{ and } \psi : F_q \to \mathbb{C}^* \text{ such that}$$
$$\chi(ab) = \chi(a)\chi(b) \text{ and } \psi(a + b) = \psi(a)\psi(b).$$

There exists a bound on arbitrary character sums by Weil [58].

i) *Multiplicative Version:* (See [24] page 225)
If m is the number of distinct roots of $f(x) \in F_q[x]$ in its splitting field over F_q, χ is a nontrivial multiplicative character of order s and $f(x)$ is not an s-th power of any polynomial, then

$$| \sum_{x \in F_q} \chi(f(x)) | \leq (m-1)q^{1/2}.$$

ii) *Additive Version* (See [24] page 223)
If $n = \deg g(x)$, $g(x) \in F_q[x]$ with $gcd(n,q) = 1$ and ψ is a nontrivial additive character of F_q, then

$$| \sum_{x \in F_q} \psi(g(x)) | \leq (n-1)q^{1/2}.$$

Stepanov gave an elementary proof of this result for the first time (See for example [45], Theorem 1, page 56).

Note that the number of affine F_q-rational points on the curves

$$y^s = f(x), \text{and}$$
$$y^p - y = g(x)$$

are

$$\sum_{\substack{\chi: \text{ multiplicative} \\ \text{character of exponent } s}} \sum_{a \in F_q} \chi(f(a)) \quad \text{and}$$
$$\sum_{\psi: \text{ additive character}} \sum_{a \in F_q} \psi(g(a))$$

respectively where p is the characteristic of F_q and $gcd(s,q) = 1$. In general if X is a smooth irreducible projective curve over F_q with N_q F_q-rational points (equivalently the algebraic function field $k(X)/F_q$ has N_q places of degree 1), then

$$N_q = q + 1 - \sum_{i=1}^{2g} \alpha_i$$

where $\alpha_i \in \mathbb{C}$ are the reciprocals of the roots of the L-polynomial of X. It is known that $| \alpha_i | = q^{1/2}$ and this is called as the *Riemann Hypothesis for Algebraic Function Fields (or Curves)*, which implies

$$| N_q - (q+1) | \leq 2gq^{1/2}.$$

Chapter 2

Codes on Hyperelliptic Curves

The purpose of this chapter is to construct long geometric Goppa codes over F_q ($q = p^\nu$, $\nu > 1$ is an odd integer). We obtain analogous results of Stepanov [47] [46] over F_q ($q = p^\nu$, $\nu > 1$ is an even integer, $p > 2$). See also [48].

2.1 The Statement of the Results

Using curves of the form

$$y_i^2 = x^{q^{1/2}} + x + c_i \quad i = 1, 2, \ldots, s$$

where $c_i \in F_{q^{1/2}}$ and $c_i \neq c_j$ if $i \neq j$, Stepanov proved the following result [47] [46].

Theorem 1 *Let $p > 2$ be a prime number, $\nu > 1$ be an even integer, and F_q be a finite field with $q = p^\nu$ elements. For any positive integer $s \leq q^{1/2}$ and $r > (sq^{1/2} - s)2^{s-2}$ there exists a geometric Goppa $[n, k, d]_q$-code C with*

$$r < n \leq (2q^{1/2} - s)q^{1/2}2^{s-1}$$

$$k \geq r - (sq^{1/2} - 3)2^{s-2}$$

$$d \geq n - r.$$

In fact he constructed curves over F_q, $q = p^\nu$, ν : even and $p > 2$ with the genus $g = (q^{1/2}s - 3)2^{s-2} + 1$ and the number of F_q-rational points $N_q \geq$

$(2q^{1/2} - s)q^{1/2}2^{s-1}$ where $s \leq q^{1/2}$. As a corollary in terms of the relative parameters R and δ he constructed codes satisfying

$$R \geq 1 - \delta - \frac{sq^{1/2} - 3}{2(2q^{1/2} - s)q^{1/2}}, \quad s \leq q^{1/2}.$$

In this chapter we prove the following Theorem.

Theorem 2 *Let $\nu > 1$ be an odd number, F_q a finite field of characteristic $p > 2$ consisting of $q = p^\nu$ elements, and s an integer such that $1 \leq s < \frac{2p^\nu + 4}{p^{(\nu-1)/2}(p+1) - 2}$. Moreover, let r be an integer satisfying*

$$2^{s-2}((p^{(\nu-1)/2}(p+1) - 2)s - 4) < r < 2^s p^\nu.$$

Then there exists a linear $[n, k, d]_q$-code with parameters

$$r < n \leq 2^s p^\nu,$$

$$k = r - 2^{s-2}((p^{(\nu-1)/2}(p+1) - 2)s - 4),$$

$$d \geq n - r.$$

Corollary 1 *Under the conditions of Theorem 2, there exists a linear $[n, k, d]_q$-code with relative parameters $R = k/n$ and $\delta = d/n$ such that*

$$R \geq 1 - \delta - \frac{2^{s-2}((p^{(\nu-1)/2}(p+1) - 2)s - 4)}{n}.$$

In particular, for $n = 2^s p^\nu$ we have

$$R \geq 1 - \delta - \frac{(p^{(\nu-1)/2}(p+1) - 2)s - 4}{4p^\nu}.$$

2.2 Proof of the Lemmas

Let $\overline{F}_q$ be an algebraic closure of the field F_q and $\mathbb{A}^{s+1}$ be $(s+1)$-dimensional affine space over $\overline{F}_q$. Morover let the characteristic of F_q be $p > 2$.

Lemma 1 *Let $f_1, f_2, \ldots, f_s \in F_q[x]$ be pairwise coprime square-free monic polynomials of the same degree $m \geq 3$ and Y be the complete intersection in $\mathbb{A}^{s+1}$ given over $F_q[x]$ via*

$$Y: \quad \begin{aligned} z_1^2 &= f_1(x), \\ z_2^2 &= f_2(x), \\ &\vdots \\ z_s^2 &= f_s(x). \end{aligned}$$

Then the genus $g = g(Y)$ of the curve Y is

$$g = \begin{cases} (ms-3)2^{s-2}+1 & \text{if } m \text{ is odd} \\ (ms-4)2^{s-2}+1 & \text{if } m \text{ is even.} \end{cases}$$

PROOF. Let I be the ideal of the curve Y in $\overline{F}_q[x, z_1 \ldots, z_s]$ and $\overline{Y}$ be the projective closure of Y in $\mathbb{P}^{s+1}$. The homogeneous ideal of $\overline{Y}$ in $\overline{F}_q[x_0, x, z_1, \ldots, z_s]$ has the form $I_h = \{f_h \mid f \in I\}$, where f_h is the homogenization of f, i.e. $f_h(x_0, x, z_1, \ldots, z_s) = f(x/x_0, z_1/x_0, \ldots, z_s/x_0)x_0^{\deg f}$. Thus $\overline{Y} = Y \cup \{(0, 0, \pm 1, \pm 1, \ldots, \pm 1)\}$ as a set, and the curve $\overline{Y}$ is singular at 2^{s-1} points $P_i \in \{(0, 0, 1, \pm 1, \ldots, \pm 1)\}$ in general.

Let X be a normalization of $\overline{Y}$ which in the same time is a non-singular model of $\overline{Y}$ (see for example Shafarevich [40] Chapter 2, 5.3). There exists a finite morphism (regular map) $\phi_1 : X \to \overline{Y}$ and composition of ϕ_1 with ϕ_2, where $\phi_2 : \overline{Y} \to \mathbb{P}^1$ via $(x_0, x, z_1, \ldots, z_s) \mapsto (x_0, x)$ gives a morphism $\phi : X \to \mathbb{P}^1$ of degree 2^s (see for example [40] Chapter 2, 3.1). Since $\overline{Y}$ has 2^{s-1} points P_i, $1 \leq i \leq 2^{s-1}$, at the hypersurface $x_0 = 0$ then $\phi^{-1}(0, 1)$ consists of 2^s or 2^{s-1} points $\{Q_i\} \subseteq X$.

Let $\Omega[\overline{Y}]$ be the space of regular differential forms on $\overline{Y}$. The space $\Omega[\overline{Y}]$, considered as a $\overline{F}_q[x, z_1, \ldots, z_s]$-module, is generated by dx and dz_i, $1 \leq i \leq s$. Since $z_i^2 = f_i(x)$, the space $\Omega[\overline{Y}]$, considered as a $\overline{F}_q[x]$-module, is generated by dx and $dx/(z_{i_1} \cdots z_{i_\sigma})$, where $1 \leq i_1 < \cdots < i_\sigma \leq s$. Next, since ϕ_1 is a morphism, the space $\Omega[X]$ is a submodule of $\Omega[\overline{Y}]$, hence any differential form $\omega \in \Omega[X]$ has the form

$$\omega = F(x)dx \quad \text{or} \quad \omega = \frac{F_{i_1,\ldots,i_\sigma}(x)dx}{z_{i_1} \cdots z_{i_\sigma}}$$

with $F, F_{i_1,\ldots,i_\sigma} \in \overline{F}_q[x]$. Thus any regular differential form in $\Omega[\overline{Y}]$ is regular at any point of X, possibly except at $Q_i \in \phi^{-1}(0, 1)$.

Let x be the coordinate on $\mathbb{P}^1$, then $u = x^{-1}$ is a local parameter at the point $(0,1)$ at infinity. Since x is a rational function on $\mathbb{P}^1$, it defines the divisor $(x) \in \mathrm{Div}(\mathbb{P}^1)$. Denoting $\phi^{-1}(x) \in \overline{F}_q(X)$ by x and its divisor by (x) again, we get the pull-back divisor $(x) \in \mathrm{Div}(X)$.

Since $\phi^{-1}(0,1)$ consists of 2^s or 2^{s-1} points Q_i then $v_{Q_i}(u) = 1$ or $v_{Q_i}(u) = 2$, so $v_{Q_i}(x) = -1$ or $v_{Q_i}(x) = -2$. If $F(x)$ is a regular function on X, we have $v_{Q_i}(F(x)dx) = -(\mathrm{deg}F(x) + 2)$ or $-(2\mathrm{deg}F(x) + 3)$, respectively. Thus $F(x)dx \notin \Omega[X]$ for any $F(x) \in \overline{F}_q[X]$.

If m is even, then there are two cases:

$$\text{i)} \quad v_{Q_i}(x) = -1 \quad \text{and} \quad v_{Q_i}(z_j) = \frac{-m}{2} \quad \text{for any } j = 1, \ldots, s,$$

or

$$\text{ii)} \quad v_{Q_i}(x) = -2 \quad \text{and} \quad v_{Q_i}(z_j) = -m \quad \text{for any } j = 1, \ldots, s.$$

Since

$$v_{Q_i}\left(\frac{F_{i_1,\ldots,i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}}\right) = v_{Q_i}(x)\mathrm{deg}F_{i_1,\ldots,i_\sigma}(x) + (v_{Q_i}(x) - 1) - \sigma v_{Q_i}(z_j)$$

for any $j = 1, \ldots, s$, then

$$\text{i)} \quad v_{Q_i}\left(\frac{F_{i_1,\ldots,i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}}\right) = \frac{m\sigma}{2} - \mathrm{deg}F_{i_1,\ldots,i_\sigma}(x) - 2,$$

or

$$\text{ii)} \quad v_{Q_i}\left(\frac{F_{i_1,\ldots,i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}}\right) = m\sigma - 2\mathrm{deg}F_{i_1,\ldots,i_\sigma}(x) - 3\ ,$$

respectively. Thus,

$$\frac{F_{i_1,\ldots,i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}} \in \Omega[X]$$

if and only if

$$\text{i)} \quad \mathrm{deg}F_{i_1,\ldots,i_\sigma}(x) \leq \frac{m\sigma}{2} - 2,$$

or

$$\text{ii)} \quad \mathrm{deg}F_{i_1,\ldots,i_\sigma}(x) \leq \frac{m\sigma}{2} - \frac{3}{2}\ ,$$

respectively. Since m is even ii) is equivalent to i).

If m is odd and $v_{Q_i}(x) = -1$, then $v_{Q_i}(z_j^2) = 2v_{Q_i}(z_j) = -m$ and we arrive at a contradiction. Thus only one case is possible, which is $v_{Q_i}(x) = -2$. In this case,

$$\frac{F_{i_1,\ldots,i_\sigma}(x)dx}{z_{i_1} \ldots z_{i_\sigma}} \in \Omega[X]$$

if only

$$\deg F_{i_1,\ldots,i_\sigma}(x) \leq \begin{cases} \dfrac{m\sigma-4}{2} & \text{if } \sigma \text{ is even,} \\ \dfrac{m\sigma-3}{2} & \text{if } \sigma \text{ is odd.} \end{cases}$$

Since X is non-singular we have $g = \dim_{\overline{F_q}} \Omega[X]$. Thus if m is even then

$$g = \frac{1}{2}\sum_{\sigma=1}^{s} \sum_{1\leq i_1<i_2,\ldots<i_\sigma\leq s} (m\sigma-2)$$

$$= (ms-4)2^{s-2}+1\ ,$$

and if m is odd then

$$g = \frac{1}{2}\sum_{\substack{\sigma=1 \\ \sigma:odd}}^{s} \sum_{1\leq i_1<i_2,\ldots<i_\sigma\leq s} (m\sigma-2) + \frac{1}{2}\sum_{\substack{\sigma=1 \\ \sigma:odd}}^{s} \sum_{1\leq i_1<i_2,\ldots<i_\sigma\leq s} (m\sigma-1)$$

$$= (ms-3)2^{s-2}+1.$$

This completes the proof. ∎

Lemma 2 *Let $\nu > 1$ be an odd number, F_q a finite field of characteristic $p > 2$ with $q = p^\nu$ elements and $f \in F_q[x]$ the polynomial*

$$f(x) = (x + x^{p^{(\nu-1)/2}})(x + x^{p^{(\nu+1)/2}}).$$

If c is a non-zero element of F_q, then the polynomials $f(x)$ and $f(x+c)$ are relatively prime.

PROOF. Let $\mu = \frac{\nu-1}{2}$ and $f'(x) = x^{p^\mu} + x$, $f''(x) = x^{p^{\mu+1}} + x$, so that $f'(x)f''(x) = f(x)$. We shall prove that $(f'(x), f'(x+c)) = (1)$ and $(f'(x), f''(x+c)) = (1)$ for any $c \in F_{p^\nu}^*$. This will imply $(f(x), f(x+c)) = (1)$ for any $c \in F_{p^\nu}^*$.

Observe that the principal ideal I' generated by $f'(x)$ and $f'(x+c)$ is

$$I' = (x^{p^\mu} + x, x^{p^\mu} + x + c^{p^\mu} + c)\ .$$

The equation

$$\alpha^{p^\mu} + \alpha = 0 \tag{1.1}$$

has no solution in $F_{p^\nu}^*$. Otherwise $\alpha^{p^\mu-1} = -1$. Then $\alpha^{p^{2\mu}-1} = 1$, since p is odd and hence $2 \mid (p^\mu + 1)$. Thus $\alpha \in F_{p^{gcd(2\mu+1,2\mu)}} = Fp$. This implies $\alpha^{p^\mu-1} = 1 \neq -1$, a contradiction.

Observe (using the Euclidean algorithm) that if $k \geq l$ are positive integers, and $c \in F_{p^\nu}$, then the principal ideal $(x^k + x + c, x^l + x)$ in $F_{p^\nu}[x]$ satisfies

$$(x^k + x + c, x^l + x) = (x^l + x, -x^{k-l+1} + x + c) \ .$$

Similarly,

$$(-x^k + x + c, x^l + x) = (x^l + x, x^{k-l+1} + x + c).$$

Combining these we find that if $k \geq 2l - 1$ and k, l are positive integers, then

$$(x^k + x + c, x^l + x) = (x^l + x, x^{k-2l+2} + x + c) \ .$$

By induction, if $l|k$ and $c \in F_{p^\nu}^*$, then

$$(x^k + x + c, x^l + x) = (x^l + x, (-1)^{k/l} x^{k/l} + x + c).$$

Applying this for $k = p^{\mu+1}$ and $l = p^\mu$ we find for the ideal $I'' = (f''(x + c), f'(x))$ that

$$I'' = (x^{p^\mu} + x, -x^p + x + c^{p^{\mu+1}} + c).$$

Now we observe that $(g'(x), g''(x)) \supset (g'(x), (g''(x))^p)$ for any $h', h'' \in F_{p^\nu}[x]$. Then

$$I'' \supset J = (x^{p^\mu} + x, -x^{p^{\mu+1}} + x^{p^\mu} + \gamma^{p^{\mu+1}} + \gamma)$$

where $\gamma = c^{p^\mu}$. We can simplify the generators of J as

$$\begin{aligned} J &= (x^{p^\mu} + x, -x^{p^{\mu+1}} - x + \gamma^{p^{\mu+1}} + \gamma) \\ &= (x^{p^\mu} + x, x^{p^{\mu+1}} + x - \gamma^{p^{\mu+1}} - \gamma). \end{aligned}$$

Let us show that

$$c^{p^{\mu+1}} + c \neq -\gamma^{p^{\mu+1}} - \gamma \ . \tag{1.2}$$

Since $\gamma = c^{p^\mu}$ and $c^{p^\nu} = c \in F_{p^\nu}^*$, we can rewrite the inequality (1.2) in the form

$$c^{p^{\mu+1}} + c^{p^\mu} + 2c \neq 0 \ . \tag{1.3}$$

The equation

$$\beta^{p^{\mu+1}} + \beta^{p^\mu} + 2\beta = 0 \tag{1.4}$$

has no solution in $F^*_{p^\nu}$. Indeed, rising both sides of (1.4) to p^μ-th power we obtain

$$\beta + \beta^{p^{2\mu}} + \beta^{p^\mu} + \beta^{p^\mu} = (\beta^{p^\mu} + \beta)^{p^\mu} + (\beta^{p^\mu} + \beta) = 0 \ . \tag{1.5}$$

Since (1.1) has no non-zero solution the last equation also has no solution in $F^*_{p^\nu}$.

Now since $f''(x+c) = x^{p^{\mu+1}} + x + c^{p^{\mu+1}} + c \in I''$, $x^{p^{\mu+1}} + x - \gamma^{p^{\mu+1}} - \gamma \in J \subseteq I''$ and

$$c^{p^{\mu+1}} + c \neq -\gamma^{p^{\mu+1}} - \gamma$$

we conclude that $I'' = (1)$.

By symmetry $(f''(x), f''(x+c)) = (1)$, and $(f''(x), f'(x+c)) = (1)$. Using uniqueness of the factorization in $F_{p^\nu}[x]$ we find that $(f'(x), f'(x+c)f''(x+c)) = (1)$, $(f''(x), f'(x+c)f''(x+c)) = (1)$, and hence $(f(x), f(x+c)) = (1)$. ∎

Let $\theta : F_q \to F_q$ be the Frobenius automorphism of F_q over F_p : $\theta(x) = x^p$. Let χ be a multiplicative character of F_p. We denote by χ_ν the character of F_q induced by χ:

$$\chi_\nu(x) = \chi(norm_\nu(x)) \ \text{ for all } x \in F_q$$

where $\mathrm{norm}_\nu(x) = x\theta(x)\dots\theta^{\nu-1}(x) = xx^p\dots x^{p^{\nu-1}}$. It easy to see that if p and ν are odd numbers, χ_ν is induced by the non-trivial quadratic character of F_p and $f(x) = (x + x^{p^{(\nu-1)/2}})(x + x^{p^{(\nu+1)/2}})$, then

$$\chi_\nu(f(x)) = \begin{cases} 1 & \text{if } x \in F_q^* \\ 0 & \text{if } x = 0 \end{cases}$$

(See [47] Lemma 2). Let

$$\tilde{f}(x) = \frac{f(x)}{x^2} = (1 + x^{p^{(\nu-1)/2-1}})(1 + x^{p^{(\nu+1)/2-1}}) \ .$$

Then $\chi_\nu(\tilde{f}(x)) = 1$ for all $x \in F_q$, and we have the following result.

Lemma 3 *Let $\nu > 1$ be an odd integer, F_q a finite field of characteristic $p > 2$ with $q = p^\nu$ elements, $c_1, \dots, c_s$ distinct elements of F_q and N_q the number of F_q-rational points of the curve Y defined by*

$$Y : \quad \begin{aligned} z_1^2 &= f_1(x) = \tilde{f}(x + c_1), \\ z_2^2 &= f_2(x) = \tilde{f}(x + c_2), \\ &\vdots \\ z_s^2 &= f_s(x) = \tilde{f}(x + c_s). \end{aligned}$$

Then

$$N_q = 2^s q.$$

PROOF. Since $\chi_\nu(f_i(x)) = \chi_\nu(\tilde{f}(x + c_i)) = 1$ for all $x \in F_{p^\nu}$, $i = 1, \ldots, s$, then we have

$$\begin{aligned} N_q &= \sum_{x \in F_{p^\nu}} (1 + \chi_\nu(f_1(x))) \ldots (1 + \chi_\nu(f_s(x))) \\ &= \sum_{x \in F_{p^\nu}} 2^s = 2^s p^\nu \end{aligned}$$

∎

2.3 Proof of Theorem 2

Consider the curve

$$Y: \quad z_i^2 = f_i(x) = \tilde{f}(x + c_i), \qquad 1 \leq i \leq s,$$

where $c_1, \ldots, c_s$ are distinct elements of F_q. The number of F_q-rational points of Y is $N_q = 2^s q$ by Lemma 3. The curve Y satisfies the conditions of Lemma 1, so its genus is

$$g = g(Y) = 2^{s-2}((p^{(\nu-1)/2}(p+1) - 2)s - 4) + 1.$$

Let S be the set of rational points on Y and $S_1 \subset S$ a subset of S. Applying Goppa's construction to

$$D_0 = \sum_{P \in S_1} P$$

and

$$D = rP_\infty$$

where $r < \deg D_0 = \mid S_1 \mid$ and P_∞ is a point of non-singular model corresponding to a point at infinity of the projectivization of the affine model Y, we get $r < n \leq 2^s p^\nu$, $k \geq r + 1 - g$, $d \geq n - r$. Since in our case also $2g - 2 < r = \deg D < n$, then $k = r + 1 - g$.

Chapter 3

Codes on Superelliptic Curves

The purpose of this chapter is to construct Goppa codes on some superelliptic curves and fibre products of them. See also [35], [36], [49].

3.1 Codes on Some Superelliptic Curves

S.A. Stepanov [43] proved the existence of a square-free polynomial $f(x) \in F_p[x]$ of degree $\geq 2(\frac{(N+1)\log 2}{\log p} + 1)$ for which

$$\sum_{i=1}^{N}(\frac{f(i)}{p}) = N$$

where $\{1, \ldots, N\} \subset F_p$ and $(\frac{\cdot}{p})$ is the Legendre symbol and $(p, 2) = 1$. Later F. Özbudak [34] extended this to arbitrary non-trivial characters of arbitrary finite fields by following Stepanov's approach. This gives a constructable proof of the fact that Weil's estimate (see Section 1.4) is almost attainable for any F_q.

Theorem 3 *Let F_q be a finite field of characteristic p, s an integer $s \geq 2$, $s \mid (q-1)$, and c be the infimum of the set*

$$C = \{x : \text{a non-negative real number} \mid \text{there exists an integer } n \text{ such that } \frac{q^x(q-2)}{(q-1)(s-1)(1+\frac{1}{sq(s-1)})} \geq n \geq \frac{q\log s}{\log q} + x\}.$$

Let r be an integer satisfying

$$s(s-1)\lceil \frac{q\log s}{\log q} + c\rceil - 2s < r < sq.$$

Then there exists a linear code $[n, k, d]_q$ *with parameters*

$$\begin{aligned} n &= sq, \\ k &= r - \tfrac{s(s-1)}{2}\lceil \tfrac{q \log s}{\log q} + c \rceil + s, \\ d &\geq sq - r. \end{aligned}$$

Therefore the relative parameters $R = \frac{k}{n}$ *and* $\delta = \frac{d}{n}$ *satisfy*

$$R \geq 1 - \delta - \frac{\frac{s(s-1)}{2}\lceil \frac{q \log s}{\log q} + c \rceil - s}{sq}.$$

Remark 1 *This result is significant especially when* q *is prime. The number of* F_q*-rational affine points in* $\mathbb{A}^2_{F_q}$ *of the curve* $y^s = f(x)$ *is* $N_q = sq$*, the genus of the curve is* $g = \frac{s(s-1)}{2}\lceil \frac{q \log s}{\log q} + c \rceil - s + 1$ *and* $\frac{N_q}{g} \sim \frac{2 \log q}{(s-1) \log s}$*. If* F_q *is not a prime field, using Galois structure of* F_q *over a proper subfield* $F_{q'} \subsetneq F_q$*, we get much larger* $\frac{N_q}{g}$ *ratios (see Theorem 4). Note that the length of the codes are* $sq > q$*.*

In [42], Stepanov introduced some special sums $S_\nu(f) = \sum_{x \in F_{q^\nu}} \chi(f(x))$ with a non-trivial quadratic character χ by explicitly representing the polynomial $f(x)$ whose absolute values are very close to Weil's upper bound. M. Glukhov [17], [18] generalized Stepanov's approach to the case of arbitrary multiplicative characters over arbitrary finite field F_q.

Firstly we apply the Goppa construction to the curve given over F_q by

$$y^s = f(x)$$

where $s \mid (q-1)$ and the polynomial $f(x)$ is obtained by Stepanov's approach to attain

$$\sum_{x \in F_q} \chi(f(x)) = q,$$

where χ is a non-trivial multiplicative character of exponent s. Moreover we apply the Goppa construction also to the polynomials $f(x)$ given in Glukhov's papers [17], [18] explicitly after some modification.

Theorem 4 *Let* F_q *be a finite field of characteristic* p*,* F_{q^ν} *an extension of* F_q *of degree* ν*,* s *an integer* $s \geq 2$*,* $s \mid (q-1)$*. Moreover*

i) if $p \neq 2$, $\nu > 1$ an odd integer and r an integer satisfying

$$(s-1)(1+q)q^{\frac{\nu-1}{2}} - 4s + 2 < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^\nu}$ with parameters

$$\begin{aligned} n &= sq^{\nu}, \\ k &= r + 2s - (s-1)\tfrac{(1+q)}{2}q^{\frac{\nu-1}{2}} - 1, \\ d &\geq sq^{\nu} - r; \end{aligned}$$

ii) if $p \neq 2$, $\nu > 2$ an even integer and r an integer satisfying

a) when $4 \not| \nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 4s + 2 < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^\nu}$ with parameters

$$\begin{aligned} n &= sq^{\nu}, \\ k &= r + 2s - (s-1)\tfrac{(1+q^2)}{2}q^{\frac{\nu}{2}-1} - 1, \\ d &\geq sq^{\nu} - r; \end{aligned}$$

b) when $4 \mid \nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 2(s-1)q - 2s < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^\nu}$ with parameters

$$\begin{aligned} n &= sq^{\nu}, \\ k &= r + (s-1)q + s - (s-1)\tfrac{(1+q^2)}{2}q^{\frac{\nu}{2}-1}, \\ d &\geq sq^{\nu} - r; \end{aligned}$$

iii) if $p = 2$, $\nu > 1$ an odd integer and r an integer satisfying

$$(s-1)(1+q)q^{\frac{\nu-1}{2}} - 2(s-1)q - 2s < r < sq^{\nu},$$

then there exists a linear code $[n,k,d]_{q^\nu}$ with parameters

$$\begin{aligned} n &= sq^{\nu}, \\ k &= r + (s-1)q + s - (s-1)\tfrac{(1+q)q^{\frac{\nu-1}{2}}}{2}, \\ d &\geq sq^{\nu} - r; \end{aligned}$$

iv) if $p = 2$, $\nu > 2$ an even integer and r an integer satisfying

a) when $4 \not| \nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 2(s-1)q^2 - 2s < r < sq^\nu,$$

then there exists a linear code $[n,k,d]_{q^\nu}$ *with parameters*

$$\begin{aligned} n &= sq^\nu, \\ k &= r + (s-1)q^2 + s - (s-1)(1+q^2)\tfrac{q^{\frac{\nu}{2}-1}}{2}, \\ d &\geq sq^\nu - r; \end{aligned}$$

b) when $4 \mid \nu$

$$(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - 2(s-1)q - 2s < r < sq^\nu,$$

then there exists a linear code $[n,k,d]_{q^\nu}$ *with parameters*

$$\begin{aligned} n &= sq^\nu, \\ k &= r + (s-1)q + s - (s-1)(1+q^2)\tfrac{q^{\frac{\nu}{2}-1}}{2}, \\ d &\geq sq^\nu - r. \end{aligned}$$

Corollary 2 *Under the same conditions with Theorem* 3, *there exists codes with relative parameters satisfying respectively*

i)

$$R \geq 1 - \delta - \frac{(s-1)\frac{(1+q)}{2}q^{\frac{\nu-1}{2}} - 2s + 1}{sq^\nu},$$

ii.a)

$$R \geq 1 - \delta - \frac{(s-1)\frac{(1+q^2)}{2}q^{\frac{\nu}{2}-1} - 2s + 1}{sq^\nu},$$

ii.b)

$$R \geq 1 - \delta - \frac{(s-1)\frac{(1+q^2)}{2}q^{\frac{\nu}{2}-1} - (s-1)q - s}{sq^\nu},$$

iii)

$$R \geq 1 - \delta - \frac{(s-1)(1+q)\frac{q^{\frac{\nu-1}{2}}}{2} - (s-1)q - s}{sq^\nu},$$

iv.a)

$$R \geq 1 - \delta - \frac{(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - (s-1)q^2 - s}{sq^\nu},$$

iv.b)

$$R \geq 1 - \delta - \frac{(s-1)(1+q^2)q^{\frac{\nu}{2}-1} - (s-1)q - s}{sq^\nu}.$$

Remark 2 *The parameters of Theorem 4 are rather good. Moreover it is possible to calculate the minimum distance d exactly in some cases directly. For example we have such codes which are near to Singleton bound:*

i: Over $F_{27} \supset F_3$ *if* $6 < r < 54$, *then it gives* $[54, r-3, d]_{27}$ *code where* $d \geq 54 - r$. *If r: even, then* $d = 54 - r$ *(see Stichtenoth [50], Remark 2.2.5).*

ii.a: Over $F_{729} \supset F_3$ *if* $84 < r < 1458$, *then it gives* $[1458, r-42, d]_{729}$ *code where* $d \geq 1458 - r$. *If r: even, then* $d = 1458 - r$.

ii.b: Over $F_{81} \supset F_3$ *if* $20 < r < 162$, *then it gives* $[162, r-10, d]_{81}$ *code where* $d \geq 162 - r$. *If r: even, then* $d = 162 - r$.

iii: Over $F_{64} \supset F_4$ *if* $18 < r < 192$, *then it gives* $[192, r-9, d]_{64}$ *code where* $d \geq 192 - r$. *If* $r \equiv 0 \ mod\ 3$, *then* $d = 192 - r$.

iv.a: Over $F_{4096} \supset F_4$ *if* $474 < r < 12288$, *then it gives* $[12288, r-237, d]_{4096}$ *code where* $d \geq 12288 - r$. *If* $r \equiv 0 \ mod\ 3$, *then* $d = 12288 - r$.

iv.b: Over $F_{256} \supset F_4$ *if* $114 < r < 768$, *then it gives* $[768, r-57, d]_{256}$ *code where* $d \geq 768 - r$. *If* $r \equiv 0 \ mod\ 3$, *then* $d = 768 - r$.

For ν*: even there are Hermitian codes (see for example Stichtenoth [50], section 7.4) which are maximal. Theorem 2 provides codes with parameters near to the parameters of maximal curves in these cases.*

3.2 Proof of Theorem 3

Let χ be a multiplicative character of exponent s of F_q. If $m \geq \frac{q \log s}{\log q} + c$, then $\frac{1}{m} q^m \frac{q-2}{q-1} \geq (s-1)s^q + 1$. Note that the number of monic irreducible

polynomials of degree m over F_q is $\frac{1}{m}\sum_{d|m}\mu(d)q^{m/d} = \frac{1}{m}q^m c_m$ (see for example [24] page 93). Here $1 \geq c_m \geq 1 - \frac{q^m - q}{q^m(q-1)} \geq \frac{q-2}{q-1}$. Forming q-tuples for each irreducible monic polynomial as in Stepanov [43] or Özbudak [34]; by Dirichlet's pigeon-hole principle if $\frac{1}{m}q^m\frac{q-2}{q-1} \geq (s-1)s^q + 1$, there exists a square-free polynomial $f \in F_q[x]$ of degree $\leq ms$ such that $\chi(f(a)) = 1$ for each $a \in F_q$. Let $\deg f = s\lceil\frac{q\log s}{\log q} + c\rceil$.

Since $s \mid (q-1)$ there are s many multiplicative characters of exponent s over F_q. Moreover for any χ of exponent s, $\chi(f(a)) = 1$ for all $a \in F_q$. Therefore we have over the curve

$$y^s = f(x)$$

$N_q = sq$ many affine F_q-rational points (see Schmidt [39] page 79 or Stepanov [45], p.51).

Using the well-known genus formulas for superelliptic curves (see for example Stichtenoth [50] p. 196), the geometric genus is given by

$$g = \frac{s(s-1)}{2}\lceil\frac{q\log s}{\log q} + c\rceil - s + 1.$$

Let D_0 be the divisor on the smooth model X of $y^s = f(x)$ where

$$D_0 = \sum_1^n x_i$$

By tracing the normalization of a curve one sees that the number of rational points of the non-singular model X of the curve $y^s = f(x)$ is more than the number of affine rational points of $y^s = f(x)$ (see for example Shafarevich [40], section 5.3). Thus $n = \deg D_0 \geq N_q = sq$. Let x_∞ be a point of X at infinity, $D = rP_\infty$ be the divisor of degree r and $supp\ D_0 \cap supp\ D = \emptyset$, where r to be determined. If

$$2g - 2 < r < N_q,$$

by using the Goppa construction,

$$n = N_q,\ \ k = r + 1 - g,\ \ d \geq N_q - r.$$

3.3 Proof of Theorem 4

Let $\chi_{\nu,s}(x) = \chi_s(norm_\nu(x))$ where χ_s is a non-trivial multiplicative character of F_q of exponent s, $norm_\nu = x.x^q.....x^{q^{\nu-1}}$. Therefore $\chi_{\nu,s}$ is a relative

multiplicative character of F_{q^ν} of exponent s. For $f(x) \in F_{q^\nu}[x]$ denote by $S_\nu(f)$ the sum $S_{\nu,s}(f) = \sum_{x \in F_{q^\nu}}(f(x))$.

Case(i):
There exists a polynomial $f_1(x) \in F_{q^\nu}[x]$

$$f_1(x) = (x + x^{q^{\frac{\nu-1}{2}}})^a (x + x^{q^{\frac{\nu+1}{2}}})^b$$

where $a + b = s$, $a \neq b$, and $(a, s) = 1$ such that $S_{\nu,s}(f_1) = q^\nu - 1$(Glukhov [18]).

We can write

$$f_1(x) = x^s (1 + x^{q^{\frac{\nu-1}{2}}-1})^a (1 + x^{q^{\frac{\nu+1}{2}}-1})^b.$$

Consider $y^s = f_1(x)$. This curve is birationally isomorphic to

$$y^s = f_{1,1}(x) = (1 + x^{q^{\frac{\nu-1}{2}}-1})^a (1 + x^{q^{\frac{\nu+1}{2}}-1})^b,$$

and $S_{\nu,s}(f_{1,1}) = q^\nu$. Moreover we know

1. $1 + x^m$ where $(m, q) = 1$ is a square-free polynomial over F_{q^ν},
2. If ν is odd, then $(1 + x^{q^{\frac{\nu-1}{2}}-1}, 1 + x^{q^{\frac{\nu+1}{2}}-1}) = 1$ over F_{q^ν} for $p \neq 2$.

Therefore we can apply Hurwitz genus formula (see for example Stichtenoth ([50], p. 196), hence we get

$$g = (s-1)\frac{(1+q)}{2} q^{\frac{\nu-1}{2}} - 2(s-1).$$

Over the curve $y^s = f_{1,1}(x)$ there are

$$N_{q^\nu} = \sum_{\exp\ \chi = s} \sum_{x \in F_{q^\nu}} \chi_s(f_{1,1}(x)) = q^\nu + (s-1) S_{\nu,s}(f_{1,1}) = s q^\nu$$

many affine F_{q^ν}-rational points (Stepanov [45], p.51). Therefore we get the desired result as in the proof of Theorem 1.

Case(ii):
We apply the same techniques to

$$f_2(x) = x^s (1 + x^{q^{\frac{\nu}{2}-1}-1})^a (1 + x^{q^{\frac{\nu}{2}+1}-1})^b$$

given by Glukhov [18]. Here $S_{\nu,s}(f_2) = \begin{cases} q^\nu - 1 & \text{if } 4 \nmid \nu \\ q^\nu - q & \text{if } 4 \mid \nu \end{cases}$. Moreover if $\nu \equiv 2 \bmod 4$, then $(1 + x^{q^{\frac{\nu}{2}-1}-1}, 1 + x^{q^{\frac{\nu}{2}+1}-1}) = 1$; and if $\nu \equiv 0 \bmod 4$, then

$(1+x^{q^{\frac{\nu}{2}-1}-1}, 1+x^{q^{\frac{\nu}{2}+1}-1}) = 1+x^{q-1}$ over F_{q^ν} for $p \neq 2$. If $\nu \equiv 2 \bmod 4$, similarly consider the curve

$$y^s = f_{2,2,1}(x) = (1+x^{q^{\frac{\nu}{2}-1}-1})^a (1+x^{q^{\frac{\nu}{2}+1}-1})^b$$

whose genus is

$$g = (s-1)\frac{(1+q^2)}{2} q^{\frac{\nu}{2}-1} - 2(s-1),$$

and $S_{\nu,s}(f_{2,2,1}) = q^\nu$. If $\nu \equiv 0 \bmod 4$ we can write $f_2(x)$ here as

$$f_2(x) = x^s (1+x^{q-1})^s \left(\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q-1}}\right)^a \left(\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q-1}}\right)^b.$$

$y^s = f_2(x)$ curve is birationally isomorphic to the curve

$$y^s = f_{2,2,2}(x) = \left(\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q-1}}\right)^a \left(\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q-1}}\right)^b$$

whose genus is

$$g = (s-1)\frac{(1+q^2)}{2} q^{\frac{\nu}{2}-1} - (s-1)(1+q),$$

and $S_{\nu,s}(f_{2,2,2}) = q^\nu$.

Case(iii):
We apply the same techniques except in this case we have the fact:

If $p = 2$, then $(1+x^k, 1+x^l) = 1+x^{(k,l)}$, where $1+x^k,\ 1+x^l \in F_{q^\nu}[x]$.

We can write $f_1(x)$ here as

$$f_1(x) = x^s (1+x^{q-1})^s \left(\frac{1+x^{q^{\frac{\nu-1}{2}}-1}}{1-x^{q-1}}\right)^a \left(\frac{1+x^{q^{\frac{\nu+1}{2}}-1}}{1+x^{q-1}}\right)^b.$$

$y^s = f_1(x)$ curve is birationally isomorphic to

$$y^s = f_{1,3}(x) = \left(\frac{1+x^{q^{\frac{\nu-1}{2}}-1}}{1+x^{q-1}}\right)^a \left(\frac{1+x^{q^{\frac{\nu+1}{2}}-1}}{1+x^{q-1}}\right)^b$$

curve. The genus is

$$g = (s-1)(1+q)\frac{q^{\frac{\nu-1}{2}}}{2} - (s-1)(1+q).$$

Moreover $S_{\nu,s}(f_1) = q^\nu - q$ (see [18]), then $S_{\nu,s}(f_{1,3}) = q^\nu$.

Case(iv):
We apply the same techniques as in Case(iii). We have

$$(q^{\frac{\nu}{2}-1}-1, q^{\frac{\nu}{2}+1}-1) = \begin{cases} q^2-1 & \text{if } 4 \nmid \nu, \\ q-1 & \text{if } 4 \mid \nu. \end{cases}$$

Thus when $4 \nmid \nu$, $y^s = f_2(x)$ is birationally isomorphic to

$$y^s = f_{2,4,1}(x) = (\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q^2-1}})^a (\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q^2-1}})^b$$

and the genus is

$$g = (s-1)(1+q^2)\frac{q^{\frac{\nu}{2}-1}}{2} - (s-1)(1+q^2).$$

Moreover $S_{\nu,s}(f_2) = q^\nu - q^2$ (see [18]), then $S_{\nu,s}(f_{2,4,1}) = q^\nu$.

When $4 \mid \nu$, $y^s = f_2(x)$ is birationally isomorphic to

$$y^s = f_{2,4,2}(x) = (\frac{1+x^{q^{\frac{\nu}{2}-1}-1}}{1+x^{q-1}})^a (\frac{1+x^{q^{\frac{\nu}{2}+1}-1}}{1+x^{q-1}})^b,$$

whose genus is

$$g = (s-1)(1+q^2)\frac{q^{\frac{\nu}{2}-1}}{2} - (s-1)(1+q),$$

and $S_{\nu,s}(f_2) = q^\nu - q$ (see [18]), then $S_{\nu,s}(f_{2,4,2}) = q^\nu$.

3.4 Codes on Fibre Products of Some Kummer Coverings

In this second half of the chapter we apply some polynomials for the corresponding finite fields to the fibre products of Kummer coverings

$$y_i^\mu = f_i(x), \quad 1 \le i \le s \tag{1.1}$$

where $\mu \mid (q-1)$ and we obtain the following result. Namely the polynomials we apply are $f_i(x) = f_1(x+c)$, $c \in A$, a corresponding subset of F_{q^ν}, where f_1 is given in Table 1 for the corresponding cases below.

Table 1

the field F_{q^ν}, $\nu > 2$, p: the characteristic of the field,
μ: a positive integer such that $\mu \mid (q-1)$, $\mu = \mu_1 + \mu_2$,
where μ_1, μ_2 are positive integer with $gcd(\mu, \mu_1) = 1$

Case 1	$p > 2$, v : odd	$f_1(x) = (1 + x^{q^{(\nu-1)/2}-1})^{\mu_1}(1 + x^{q^{(\nu+1)/2}-1})^{\mu_2}$
Case 2	$p > 2$, $v \equiv 2 \bmod 4$	$f_1(x) = (1 + x^{q^{\nu/2-1}-1})^{\mu_1}(1 + x^{q^{\nu/2+1}-1})^{\mu_2}$
Case 3	$p > 2$, $v \equiv 0 \bmod 4$	$f_1(x) = (\frac{1 + x^{q^{\nu/2-1}-1}}{1 + x^{q-1}})^{\mu_1}(\frac{1 + x^{q^{\nu/2+1}-1}}{1 + x^{q-1}})^{\mu_2}$
Case 4	$p = 2$, v : odd	$f_1(x) = (\frac{1 + x^{q^{(\nu-1)/2}-1}}{1 + x^{q-1}})^{\mu_1}(\frac{1 + x^{q^{(\nu+1)/2}-1}}{1 + x^{q-1}})^{\mu_2}$
Case 5	$p = 2$, $v \equiv 2 \bmod 4$	$f_1(x) = (\frac{1 + x^{q^{\nu/2-1}-1}}{1 + x^{q^2-1}})^{\mu_1}(\frac{1 + x^{q^{\nu/2+1}-1}}{1 + x^{q^2-1}})^{\mu_2}$
Case 6	$p = 2$, $v \equiv 0 \bmod 4$	$f_1(x) = (\frac{1 + x^{q^{\nu/2-1}-1}}{1 + x^{q-1}})^{\mu_1}(\frac{1 + x^{q^{\nu/2+1}-1}}{1 + x^{q-1}})^{\mu_2}$

Theorem 5 *Let $\nu > 2$ be a positive integer, F_{q^ν} a finite field of characteristic p, μ an integer $\mu \geq 2$, $\mu \mid (q-1)$. If s is an integer satisfying the corresponding conditions given in Table 2 below, then there exists $A_j \subset F_{q^\nu}$ for the respective cases $j = 1, \ldots, 6$ such that the affine curves given by (1.1) and Table 1 have $N_{q^\nu} = \mu^s q^\nu$ many affine F_{q^ν}-rational points and genera g_j as given in Table 2 below respectively.*

Therefore if r is an integer satisfying the conditions given in Table 3 below respectively, we get linear $[n, k, d]_{q^\nu}$-codes with the corresponding parameters given in Table 3. Moreover the relative parameters $R = \frac{k}{n}$ and $\delta = \frac{d}{n}$ satisfy

$$R \geq 1 - \delta - J(n, s, \mu, q)$$

where $J(n, s, \mu, q)$ is given in Table 4 respectively.

Table 2

Case $j = 1, \ldots, 6$	Conditions on s	genus, g_j, $j = 1, \ldots, 6$
Case 1 $p > 2$ ν : odd	$1 \leq s \leq \dfrac{2\mu(q^\nu + 1)}{(\mu - 1)(q^{(\nu-1)/2}(q+1) - 2)}$	$\dfrac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1) - 2) - 2\mu\Big) + 1$
Case 2 $p > 2$ $\nu \equiv 2 \bmod 4$	$1 \leq s \leq \dfrac{2\mu(q^\nu + 1)}{(\mu - 1)(q^{\nu/2-1}(q^2+1) - 2)}$	$\dfrac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1) - 2) - 2\mu\Big) + 1$
Case 3 $p > 2$ $\nu \equiv 0 \bmod 4$	$1 \leq s \leq \dfrac{2\mu(q^\nu + 1)}{(\mu - 1)(q^{\nu/2-1}(q^2+1) - 2q)}$	$\dfrac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1) - 2q) - 2\mu\Big) + 1$
Case 4 $p = 2$ ν : odd	$1 \leq s \leq \dfrac{2\mu(q^\nu + 1)}{(\mu - 1)(q^{(\nu-1)/2}(q+1) - 2q)}$	$\dfrac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1) - 2q) - 2\mu\Big) + 1$
Case 5 $p = 2$ $\nu \equiv 2 \bmod 4$	$1 \leq s \leq \dfrac{2\mu(q^\nu + 1)}{(\mu - 1)(q^{\nu/2-1}(q^2+1) - 2q^2)}$	$\dfrac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1) - 2q^2) - 2\mu\Big) + 1$
Case 6 $p = 2$ $\nu \equiv 0 \bmod 4$	$1 \leq s \leq \dfrac{2\mu(q^\nu + 1)}{(\mu - 1)(q^{\nu/2-1}(q^2+1) - 2q)}$	$\dfrac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1) - 2q) - 2\mu\Big) + 1$

Table 3

Case	Condition on r	$[n,k,d]_{q^\nu}$
Case 1 $p>2$ v : odd	$\frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1)-2)-2\mu\Big)$ $< r < \mu^s q^\nu$	$r < n \le \mu^s q^\nu$ $k \ge r - \frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1)-2)-2\mu\Big)$ $d \ge n-r$
Case 2 $p>2$ $v \equiv 2 \bmod 4$	$\frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2)-2\mu\Big)$ $< r < \mu^s q^\nu$	$r < n \le \mu^s q^\nu$ $k \ge r - \frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2)-2\mu\Big)$ $d \ge n-r$
Case 3 $p>2$ $v \equiv 0 \bmod 4$	$\frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q)-2\mu\Big)$ $< r < \mu^s q^\nu$	$r < n \le \mu^s q^\nu$ $k \ge r - \frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q)-2\mu\Big)$ $d \ge n-r$
Case 4 $p=2$ v : odd	$\frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1)-2q)-2\mu\Big)$ $< r < \mu^s q^\nu$	$r < n \le \mu^s q^\nu$ $k \ge r - \frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1)-2q)-2\mu\Big)$ $d \ge n-r$
Case 5 $p=2$ $v \equiv 2 \bmod 4$	$\frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q^2)-2\mu\Big)$ $< r < \mu^s q^\nu$	$r < n \le \mu^s q^\nu$ $k \ge r - \frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q^2)-2\mu\Big)$ $d \ge n-r$
Case 6 $p=2$ $v \equiv 0 \bmod 4$	$\frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q)-2\mu\Big)$ $< r < \mu^s q^\nu$	$r < n \le \mu^s q^\nu$ $k \ge r - \frac{\mu^{s-1}}{2}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q)-2\mu\Big)$ $d \ge n-r$

Remark 3 *The parameters of the codes of Theorem 5 are rather good. First of all the lengths are in the order of $\mu^s q^\nu$ which are far larger than q^ν =the number of elements of the field and the parameters are near to Singleton bound at the same time. It is possible to calculate the minimum distance in some cases directly. For example we have such codes:*

i) Over $F_{27} \supset F_3$ if $6 < r < 54$, then it gives $[54, r-3, d]_{27}$ code where $d \ge 54 - r$. If r is even, then $d = 54 - r$ (see Stichtenoth [50] Remark 2.2.5).

ii) Over $F_{64} \supset F_4$ if $18 < r < 192$, then it gives $[192, r-9, d]_{64}$ code where $d \ge 192 - r$. If $r \equiv 0 \bmod 3$, then $d = 192 - r$.

iii) Over $F_{1331} \supset F_{11}$ if $11600 < r < 133100$, then it gives $[133100, k, d]_{1331}$ code where $k \ge r - 11600$ and $d \ge 133100 - r$.

If $q^\nu = p^{\nu'}$ where p is the characteristic of the field and ν' is even, there exist better codes in some respects. For instance Hermitian codes (see for example [50], Example 6.4.2) which are maximal codes. Moreover the codes of Stepanov [47] are also better in this case if $p \neq 2$ and longer than Hermitian codes. However the codes of Theorem 5 are even longer than the codes of [47] if $\mu > 2$ and also includes the case $p = 2$.

If $q^\nu = p^{\nu'}$ where ν' is odd, there are not maximal codes as Hermitian codes of the case ν' : even. Van der Geer and van der Vlugt found independently good codes by fibre products of Artin-Schreier curves [16]. The results of Theorem 5 are compatible with their results. Moreover we have one more parameter μ and our codes are much longer than their codes while near to Singleton bound as close as their codes.

Theorem 5 also extends the results of [48] since $\mu = 2$ was fixed in that case. Moreover in this way we get similar results also for characteristic $p = 2$ fields.

It is known that by fibre products of Kummer coverings of the affine line, one cannot get asymptotically good curves (see [8]). This explains why s and therefore the length of the codes in Theorem 5 and the codes given by Geer-Vlugt are bounded. Recently Garcia and Stichtenoth gave a sequence of curves of arbitrarily large genera with good parameters over square finite fields using Artin-Schreier coverings [12].

Table 4

Case	$J(n,s,\mu,q)$
Case 1 $p>2$ ν : odd	$\dfrac{\mu^{s-1}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1)-2)-2\mu\Big)}{2n}$
Case 2 $p>2$ $\nu \equiv 2 \bmod 4$	$\dfrac{\mu^{s-1}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2)-2\mu\Big)}{2n}$
Case 3 $p>2$ $\nu \equiv 0 \bmod 4$	$\dfrac{\mu^{s-1}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q)-2\mu\Big)}{2n}$
Case 4 $p=2$ ν : odd	$\dfrac{\mu^{s-1}\Big((\mu-1)s(q^{(\nu-1)/2}(q+1)-2q)-2\mu\Big)}{2n}$
Case 5 $p=2$ $\nu \equiv 2 \bmod 4$	$\dfrac{\mu^{s-1}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q^2)-2\mu\Big)}{2n}$
Case 6 $p=2$ $\nu \equiv 0 \bmod 4$	$\dfrac{\mu^{s-1}\Big((\mu-1)s(q^{\nu/2-1}(q^2+1)-2q)-2\mu\Big)}{2n}$

3.5 The Calculation of the Genus

Let $\overline{F}_{q^\nu}$ be an algebraic closure of the field F_{q^ν} and $\mathbb{A}^{s+1}$ be $(s+1)$-dimensional affine space over $\overline{F}_{q^\nu}$.

Let $\theta : F_{q^\nu} \to F_{q^\nu}$ be the Frobenius automorphism of F_{q^ν} over $F_q : \theta(x) = x^q$. The multiplicative homomorphism

$$norm_\nu(x) = x.\theta(x).\theta^2(x)\ldots\theta^{\nu-1}(x) = x.x^q\ldots x^{q^{\nu-1}}$$

of the field F_{q^ν} onto F_q is the relative norm of $x \in F_{q^\nu}$ with respect to F_q. Let

χ_μ be a non-trivial multiplicative character of F_q of exponent μ, so $\mu > 1$. We denote by $\chi_{\nu,\mu}$ the multiplicative character of F_{q^ν} induced by χ_μ:

$$\chi_{\nu,\mu}(x) = \chi_\mu(norm_\nu(x)).$$

For $f(x) \in F_{q^\nu}[x]$ we denote by $S_{\nu,a}(f)$ the sum

$$S_{\nu,\mu}(f) = \sum_{x \in F_{q^\nu}} \chi_{\nu,\mu}(f(x)).$$

Lemma 4 *Let $f_{i,1}$, $f_{i,2}$, ..., $f_{i,s} \in F_q[x]$ be square-free monic polynomials of the same degree m_i for $i = 1, 2$. Let μ_1, μ_2 be positive integers, $\mu \geq 2$ a positive integer with $\mu \mid q-1$, $gcd(\mu, \mu_1) = 1$, and $m_1\mu_1 + m_2\mu_2 \geq \mu + 1$. Assume $f_{i,j}$, $i = 1, 2, \ldots, s$, $j = 1, 2$ be pairwise coprime polynomials in $F_q[x]$. Let Y be the fibre product in $\mathbb{A}^{s+1}$ given over $F_q[x]$ via*

$$\begin{aligned} & z_1^\mu = (f_{1,1}(x))^{\mu_1}(f_{1,2}(x))^{\mu_2}, \\ Y: \quad & z_2^\mu = (f_{2,1}(x))^{\mu_1}(f_{2,2}(x))^{\mu_2}, \\ & \vdots \\ & z_s^\mu = (f_{s,1}(x))^{\mu_1}(f_{s,2}(x))^{\mu_2}. \end{aligned}$$

Moreover let $m = m_1\mu_1 + m_2\mu_2$ and assume $(m, \mu) = 1$ or $(m, \mu) = \mu$. Then the genus $g = g(Y)$ of the curve Y is

$$g = \begin{cases} \dfrac{\mu^{s-1}}{2}((\mu-1)s(m_1+m_2) - (\mu+1)) + 1 & \text{if } (m,\mu) = 1 \\ \dfrac{\mu^{s-1}}{2}((\mu-1)s(m_1+m_2) - (2\mu)) + 1 & \text{if } (m,\mu) = \mu. \end{cases}$$

PROOF. The plan of the proof is as follows. First we consider the curve with $\mu_1 = \mu_2 = 1$:

$$\begin{aligned} & z_1^\mu = f_{1,1}(x)f_{1,2}(x), \\ Y: \quad & \vdots \\ & z_s^\mu = f_{s,1}(x)f_{s,2}(x). \end{aligned}$$

Note that the affine curve Y is non-singular and we compute the genus using the same methods of Lemma 1 [48]. Then we consider for general μ_1, μ_2. In this case the affine curve is singular in general. We add contributions of these singularities to the genus using Riemann-Hurwitz formula.

Now let $\mu_1 = \mu_2 = 1$. Let I be the ideal of the curve Y over $\overline{F_q}$ and $\overline{Y}$ be the projective closure of Y in $\mathbb{P}^{s+1}$. The homogeneous ideal of $\overline{Y}$ in

$\overline{F_q}[x_0, x, z_1, \ldots, z_s]$ has the form $I_h = \{f(x/x_0, z_1/x_0, \ldots, z_s/x_0)x_0^{\deg f} \mid f \in I\}$. Thus $\overline{Y} = Y \cup \{[0:0:\xi_1:\cdots:\xi_s]\}$ where $\xi^\mu = 1$ for $i = 1, \ldots, s$ and the curve $\overline{Y}$ is singular at μ^{s-1} points $P_i \in \{[0:0:\xi_1:\cdots:\xi_s]\}$ in general.

Let X be normalization of $\overline{Y}$. There exists a finite regular morphism $\phi_1 : X \to \overline{Y}$. Let $\phi_2 : \overline{Y} \to \mathbb{P}^1$ be the projection $[x_0, x : z_1 : \cdots : z_s] \to [x_0 : x]$. Then $\phi : X \to \mathbb{P}^1$ is a finite regular surjective morphism of degree μ^s where $\phi = \phi_2 \circ \phi_1$. Since $\overline{Y}$ has already μ^{s-1} points P_i, $1 \le i \le \mu^{s-1}$ at the hypersurface $x_0 = 0$, $\phi^{-1}([0:1])$ consists of μ^s or $\mu^{s-1}l$, $1 < l$, $l \mid \mu$ points call $\{Q_i\} \subset X$, by symmetry.

Let $\Omega[Y]$ be the $\overline{F_q}[x, z_1, \ldots z_s]$ module of regular differential forms generated by dx and dz_i, $1 \le i \le s$. Since $z_i^\mu = f_i(x)$ for $i = 1, 2, \ldots, s$ we have

$$\Omega[Y] = < \frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}} \mid 1 \le i_1 < i_2 \cdots < i_\sigma \le s,\ 0 \le n_{i_j} \le \mu - 1,\ j = 1, \ldots, \sigma >_{\overline{F_q}[x]}$$

since the affine curve Y is non-singular. Therefore $\Omega[X]$ is an $\overline{F_q}[x]$ submodule of $\Omega[Y]$ since ϕ is regular. Hence any differential form $\omega \in \Omega[X]$ has the form

$$\omega = F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x)\frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}},$$

where $F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x) \in \overline{F_q}[x]$. Note that any differential form $\omega \in \Omega[X]$ is non-singular at any point of X except $Q \in \phi^{-1}\{[0:1]\}$.

Let x be the coordinate on $\mathbb{P}^1$, then $u = x^{-1}$ is a local parameter at the infinity point $[0:1] \in \mathbb{P}^1$. Since x is a rational function on $\mathbb{P}^1$, it defines the divisor $(x) \in Div(\mathbb{P}^1)$. Denoting $\phi^{-1}(x) \in \overline{F_{q^\nu}}(X)$ a rational function on X by x and its divisor by (x) again, we get the pull-back divisor $(x) \in Div(X)$.

If $\mid \{Q_i\} \mid = \mid \phi^{-1}([0:1]) \mid = \mu^s$, then $v_{Q_i}(u) = 1$. If $\mid \{Q_i\} \mid = \mu^{s-1}l$, Then $v_{Q_i}(u) = d$ and $d \mid \mu$ since $\mu^s = d\mu^{s-1}l$ using the formula $\deg\phi \cdot v_{[0:1]}(u) = \sum_{Q_i} v_{Q_i}(u)$. Now there are two cases to consider in our lemma: $(\mu, m) = 1$ and $\mu \mid m$. Let $Q \in \{Q_i\}$.

Case $(\mu, m) = 1$: If $v_Q(u) = 1$, then $v_Q(x) = -1$, $v_Q(z_i^\mu) = -m$, and $v_Q(z_i) = -m/\mu \notin \mathbb{Z}$, a contradiction. Thus $v_Q(u) = d$ and $d \mid \mu$. Hence $v_Q(z_i) = -md/\mu$ and $\mu \mid d$, so $\mu = d$. In short we have

1) $v_Q(x) = -\mu$,

2) $v_Q(z_i) = -m$ for $i = 1, \ldots, s$,

3) $v_Q(dx) = -(\mu + 1)$.

In this case

$$\omega = F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x)\frac{dx}{z_{i_1}^{n_{i_1}} \cdots z_{i_\sigma}^{n_{i_\sigma}}} \in \Omega[X]$$

if and only if $v_Q(\omega) \geq 0$. This means

$$\deg F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x) \leq \frac{m(n_1+\cdots+n_{i_\sigma})-(\mu+1)}{\mu}.$$

If $m(n_{i_1}+\cdots+n_{i_\sigma})-1 \equiv k \bmod \mu$ where $k=0,1,\ldots,\mu-1$, then

$$[\frac{m(n_{i_1}+\cdots+n_{i_\sigma})-(\mu+1)}{\mu}] = \frac{m(n_{i_1+\cdots+n_{i_\sigma}})-(\mu+1)-k}{\mu},$$

where $[\,\cdot\,]$ is the greatest integer function. Therefore we have

$$\begin{aligned}&\dim_{\overline{F_{q^\nu}}}\{F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x)\frac{dx}{z_{i_1}^{n_{i_1}}\cdots z_{i_\sigma}^{n_{i_\sigma}}} \mid m(n_{i_1}+\cdots+n_{i_\sigma}) \equiv k+1 \bmod \mu\}\\ &= \frac{m(n_{i_1}+\cdots+n_{i_\sigma})-(k+1)}{\mu}.\end{aligned}$$

To calculate genus we use a generating function for partitions. Let

$$\begin{aligned}u(x) &= (1+x+\cdots+x^{\mu-1})^s = 1+c_1x+c_2x^2+\cdots+c_{(\mu-1)s}x^{(\mu-1)s}\\ &= 1+x(c_1+c_{\mu+1}x^\mu+\cdots)+x^2(c_2+c_{\mu+2}x^\mu+\cdots)+\cdots+x^\mu(c_\mu+c_{2\mu}x^\mu+\cdots).\end{aligned}$$

Let

$$\begin{aligned}L_1 &= c_1+c_{\mu+1}+\cdots,\\ L_2 &= c_2+c_{\mu+2}+\cdots,\\ &\vdots\\ L_\mu &= c_\mu+c_{2\mu}+\cdots.\end{aligned}$$

Let $\theta = e^{\frac{2\pi i}{\mu}}$. Then we have

$$\begin{aligned}u(1)-1 &= L_1+L_2+\cdots+L_\mu,\\ u(\theta)-1 &= L_1\theta+L_2\theta^2+\cdots+L_\mu\theta^\mu,\\ &\vdots\\ u(\theta^{\mu-1})-1 &= L_1\theta^{(\mu-1)}+L_2\theta^{2(\mu-1)}+\cdots+L_\mu\theta^{\mu(\mu-1)}.\end{aligned}$$

In matrix form

$$\underbrace{\begin{bmatrix}1 & 1 & & 1\\ \theta & \theta^2 & & \theta^\mu\\ \theta^2 & \theta^4 & & \theta^{2\mu}\\ \vdots & \vdots & & \vdots\\ \theta^{(\mu-1)} & \theta^{2(\mu-1)} & \ldots & \theta^{\mu(\mu-1)}\end{bmatrix}}_{A}\begin{bmatrix}L_1\\ L_2\\ L_3\\ \vdots\\ L_\mu\end{bmatrix} = \begin{bmatrix}\mu^s-1\\ -1\\ -1\\ \vdots\\ -1\end{bmatrix}.$$

Note that $A = [A_{ij}]_{\mu\times\mu} = [\theta^{(i-1)j}]$. Then $L_i = \dfrac{\triangle_i}{\triangle}$ where $\triangle = \det A$, $\triangle_i = \det A_i$ and A_i is the matrix whose ith column is interchanged with

$[\mu^s-1,-1,\ldots,-1]^T$. We have $L_1 = L_2 = \cdots = L_{\mu-1} = \mu^{s-1}$ and $L_\mu = \mu^{s-1}-1$. Similarly let

$$\begin{aligned} v(x) &= \frac{d}{dx}u(x) = s(1+x+\cdots+x^{\mu-1})^{s-1}(1+2x+3x^2+\cdots+(\mu-1)x^{\mu-2}), \\ &= c_1 + 2c_2x + 3c_3x^2 + \cdots, \\ &= (c_1 + (\mu+1)c_{\mu+1}x^\mu + \cdots) + x(2c_2 + (\mu+2)c_{\mu+2}x^\mu + \cdots) + \cdots, \end{aligned}$$

and

$$\begin{aligned} \tilde{L_1} &= c_1 + (\mu+1)c_{\mu+1} + \cdots, \\ \tilde{L_2} &= 2c_2 + (\mu+2)c_{\mu+2} + \cdots, \\ &\vdots \\ \tilde{L_\mu} &= \mu c_\mu + (2\mu)c_{2\mu} + \cdots. \end{aligned}$$

Then we have

$$\tilde{L_1} + \tilde{L_2} + \cdots \tilde{L_\mu} = v(1) = s\mu^{s-1}\frac{\mu(\mu-1)}{2}.$$

Note that

$$L_k = \sum_{\sigma=1}^{s} \sum_{1\le i_1<i_2<\cdots<i_\sigma\le s} \sum_{\substack{0\le n_{i_1}\le \mu-1 \\ 0\le n_{i_2}\le \mu-1 \\ \vdots \\ 0\le n_{i_\sigma}\le \mu-1}} \delta_k(n_{i_1},\ldots,n_{i_\sigma})$$

and

$$\tilde{L_k} = \sum_{\sigma=1}^{s} \sum_{1\le i_1<i_2<\cdots<i_\sigma\le s} \sum_{\substack{0\le n_{i_1}\le \mu-1 \\ 0\le n_{i_2}\le \mu-1 \\ \vdots \\ 0\le n_{i_\sigma}\le \mu-1}} (n_{i_1}+\cdots+n_{i_\sigma})\delta_k(n_{i_1},\ldots,n_{i_\sigma})$$

where

$$\delta_k(n_{i_1},\ldots,n_{i_\sigma}) = \begin{cases} 1 & \text{if } n_{i_1}+\cdots+n_{i_\sigma} \equiv k \bmod \mu, \\ 0 & \text{else.} \end{cases}$$

Therefore the genus of Y $g = g(Y)$ is

$$\begin{aligned} g &= \frac{m}{\mu}\sum_{k=1}^{\mu-1}\tilde{L_k} - \frac{1}{\mu}\sum_{k=1}^{\mu-1}kL_k + \frac{m}{\mu}\tilde{L_\mu} - \frac{\mu}{\mu}L_\mu \\ &= \frac{m}{\mu}s\mu^s\frac{\mu-1}{2} - \frac{1}{\mu}\sum_{k=1}^{\mu-1}k\mu^{s-1} - \frac{\mu}{\mu}(\mu^{s-1}-1) \\ &= \frac{ms\mu^{s-1}(\mu-1)}{2} - \frac{1}{\mu}\sum_{k=1}^{\mu}k\mu^{s-1} + 1 \\ &= \frac{ms\mu^{s-1}(\mu-1)}{2} - \frac{1}{\mu}\mu^{s-1}\frac{\mu(\mu+1)}{2} + 1 \\ &= \frac{\mu^{s-1}}{2}(ms(\mu-1)-(\mu+1)) + 1. \end{aligned}$$

Case $\mu \mid m$: In this case we have

1) $v_Q(x) = \frac{-\mu}{l}$,

2) $v_Q(z_i) = \frac{-m}{l}$ for $i = 1, 2, \ldots, s$,

3) $v_Q(dx) = -(\frac{\mu}{l} + 1)$,

where $l = \mu/d$. Therefore

$$\omega = F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x)\frac{dx}{z_{i_1}^{n_{i_1}}\cdots z_{i_\sigma}^{n_{i_\sigma}}} \in \Omega[X]$$

if and only if

$$\deg F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x) \leq \frac{m}{\mu}(n_{i_1}+\cdots+n_{i_\sigma}) - 2.$$

Thus

$$\begin{aligned} &\dim_{\overline{F_{q^\nu}}}\{F_{(i_1,n_{i_1}),\ldots,(i_\sigma,n_{i_\sigma})}(x)\frac{dx}{z_{i_1}^{n_{i_1}}\cdots z_{i_\sigma}^{n_{i_\sigma}}} \in \Omega[X]\} \\ &= \frac{m}{\mu}(n_{i_1}+\cdots+n_{i_\sigma}) - 1. \end{aligned}$$

Therefore the genus $g = g(Y)$ is

$$\begin{aligned} g &= \frac{m}{\mu}\sum_{k=1}^{\mu}\tilde{L_k} - \sum_{k=1}^{\mu}L_k \\ &= \frac{m}{\mu}(s\frac{\mu^s(\mu-1)}{2}) - (\mu\mu^{s-1}-1) \\ &= \frac{\mu^{s-1}}{2}(ms(\mu-1)-2\mu) + 1. \end{aligned}$$

Now we can compute the genus for general (μ_1, μ_2) using Riemann-Hurwitz formula. Recall that if $\phi : X \to \mathbb{P}^1$ is a finite regular morphism of projective irreducible curves, then

$$g(X) = 1 + \frac{1}{2} \sum_{P \in X \setminus \phi^{-1}([0:1])} (e_P - 1) + \frac{1}{2} \sum_{Q \in \phi^{-1}([0:1])} (e_Q - 1) - \deg\phi$$

where e_P and e_Q are ramification indices of ϕ at P and Q respectively. Let

$$Y_1 : \begin{array}{c} z_1^{\mu} = f_{1,1}(x)^{\mu_1} f_{1,2}(x)^{\mu_2} \\ \vdots \\ z_s^{\mu} = f_{s,1}(x)^{\mu_1} f_{s,2}(x)^{\mu_2} \end{array}$$

be the general form of the curve that we want to calculate its genus. Let

$$Y_2 : \begin{array}{c} z_1^{\mu} = f_1 \\ \\ z_s^{\mu} = f_s \end{array}$$

be the curve where $\mu_1 = \mu_2 = 1$ and $m = \deg f_i$ for $i = 1, \ldots, s$, f_i are pairwise coprime. If X_i is the normalization of the projectivization of Y_i and $\phi_i \to \mathbb{P}^1$ the corresponding maps, then $\deg\phi_i = \mu^s$, $i = 1, 2$. Moreover

$$\sum_{Q \in \phi_1^{-1}([0:1])} (e_Q - 1) = \sum_{Q \in \phi_2^{-1}([0:1])} (e_Q - 1)$$

since $m = \deg f_i$, $i = 1, \ldots, s$. Consider the curve Y_1. If $\phi_1(P) = [1, t]$, $t \in \overline{F}_{q^\nu}$ and $(f_{1,1}(t)f_{1,2}(t)) \ldots (f_{s,1}(t)f_{s,2}(t)) \neq 0$, then $\mid \phi_1^{-1}([1, t]) \mid = \mu^s$ and $e_P = 1$ for each $P \in \phi_1^{-1}([1 : t])$. If $\phi_1(P) = [1, t]$ and $f_{1,1}(t) = 0$, then $(f_{1,2}(t))(f_{2,1}(t)f_{2,2}(t)) \ldots (f_{s,1}(t)f_{s,2}(t)) \neq 0$ since they are relatively prime polynomials. Therefore $\mid \phi_1^{-1}([1 : t]) \mid = \mu^{s-1}$ and $e_P = \mu$ for each $P \in \phi^{-1}([1 : t])$. This holds for other polynomials also. Therefore

$$\sum_{P \in X_1 \setminus \phi_1^{-1}([0:1])} (e_P - 1) = s(m_1 + m_2)(\mu - 1)\mu^{s-1}.$$

Similarly for Y_2 we have

$$\sum_{P \in X_2 \setminus \phi_2^{-1}([0:1])} (e_P - 1) = sm(\mu - 1)\mu^{s-1}.$$

Therefore if we denote genus of Y_i by g_i, $i = 1, 2$ we have

$$g_1 = g_2 + \frac{s(m_1 + m_2)(\mu - 1)\mu^{s-1}}{2} - \frac{sm(\mu - 1)\mu^{s-1}}{2}.$$

But we know

$$g_2 = \begin{cases} \frac{\mu^{s-1}}{2}((\mu-1)sm-(\mu+1))+1 & \text{if } (m,\mu)=1, \\ \frac{\mu^{s-1}}{2}((\mu-1)sm-2\mu)+1 & \text{if } (m,\mu)=\mu. \end{cases}$$

Adding the difference we prove the lemma. ∎

Remark 4 *Note that there exists a different method to calculate the genus given by Xing [56]. Our method, which is a generalization of that of Stepanov's, allows us to find explicitly a basis for regular differential forms on the curve. Moreover this provides a fast decoding algorithm following the arguments of the proof of Lemma 4 after the resolution of affine singularities.*

3.6 The Calculation of The Number of F_{q^ν}-rational Points

Lemma 5 *Let $\nu > 1$ be an integer, F_{q^ν} a finite field of characteristic p, $\mu \geq 2$ an integer, $\mu \mid (q-1)$, μ_1, μ_2 positive integers with $\mu_1+\mu_2 = \mu$ and $gcd(\mu,\mu_1) = 1$. Then there exist $A_j \subset F_{q^\nu}$ for the cases $j = 1,\ldots,6$ corresponding to the Table 1 such that the curve Y defined by*

$$Y: \ z_i^\mu = f_1(x+c_i),\ 1 \leq i \leq s$$

where f_1 is defined in Table 1, $s \leq |A_j|$ is absolutely irreducible and it has $\mu^s q^\nu$ many F_{q^ν}-rational affine points in $\mathbb{A}^{s+1}_{F_{q^\nu}}$. Moreover $|A_j| = q^\nu$ for $j = 1,2$, $|A_4| = q^{\nu-1}$, and $|A_j| = q^{\nu-2}$ for $j = 3,5,6$.

PROOF. The proofs are similar for all six cases. We give the proof for the Case 3, i.e. $p > 2$, $\nu \equiv 0 \bmod 4$. $f_1(x) = (\frac{1+x^{q^{\nu/2-1}}-1}{1+x^{q-1}})^{\mu_1}(\frac{1+x^{q^{\nu/2+1}-1}}{1+x^{q-1}})^{\mu_2}$ in this case.

Let $g_1(x) = (x^{q^{\nu/2-1}} + x)$ and $H_1 = \{c \in F_{q^\nu} \mid c^{q^{\nu/2-1}} + c = 0\}$. Observe that H_1 is an additive subgroup of F_{q^ν} with $H_1 = \{0\} \cup \{g^{\frac{2s+1}{2}(q+1)} \mid 0 \leq s \leq q-2,\ g \text{ is a generator of } F^*_{q^2}\}$ and $gcd(g_1(x), g_1(x+c)) = 1$ for $c \in F_{q^\nu} \setminus H_1$.

Let $g_2(x) = (x^{q^{\nu/2+1}} + x)$. Then $gcd(g_2(x), g_2(x+c)) = 1$ for $c \in F_{q^\nu} \setminus H_1$ similarly.

Let $\delta = \frac{\nu}{2} - 1$ and I be the ideal of $F_{q^\nu}[x]$ defined by $I = (g_2(x+c), g_1(x))$ where $c \in F_{q^\nu}$. Using Euclidean algorithm we get $I = (x^{q^\delta} + x, -x^{q^2} + x +$

$c^{q^{\delta+2}}+c$) (see the proof of Lemma 2 in [48]). Moreover if $J=(x^{q^\delta}+x, -x^{q^{\delta+2}}+x^{q^\delta}+c_1^{q^{\delta+2}}+c_1)$ where $c_1=c^{q^\delta}$, then

$$I \supset J = (x^{q^\delta}+x, x^{q^{\delta+2}}+x-c_1^{q^{\delta+2}}-c_1).$$

Since $g_2(x+c)\in I$, if

$$c^{q^{\delta+2}}+c+c_1^{q^{\delta+2}}+c_1 \neq 0, \tag{1.2}$$

then $I=(1)$. But (1.2) holds iff

$$(c^{q^{\delta+2}}+c+c_1^{q^{\delta+2}}+c_1)^{q^\delta} = (c^{q^\delta}+c)^{q^\delta}+(c^{q^\delta}+c) \neq 0. \tag{1.3}$$

Let τ be the additive homomorphism defined by

$$\tau : F_{q^\nu} \to F_{q^\nu}, \quad \tau(c) = c^{q^\delta}+c.$$

Then $ker\tau = H_1$. Let $H_2=\tau^{-1}(H_1)$ be the inverse image of H_1. H_2 is again an additive subgroup of F_{q^ν} and $|H_2|=|H_1||ker\tau|= q^2$. The inequality (1.3) is satisfied when $c \notin F_{q^\nu} \setminus H_2$. Then A_3 is a complete set of representatives of F_{q^ν}/H_2. Therefore $gcd(f_1(x+c), f_1(x)) = 1$ over $F_{q^\nu}[x]$ in this case and Y is absolutely irreducible.

By similar arguments we find $A_1 = A_2 = F_{q^\nu}^*$, A_4 as a complete set of representatives of F^{q^ν}/F_q, and $A_5 = A_6$ as a complete set of representatives of F_{q^ν}/F_{q^2}.

Let χ be any non-trivial multiplicative character of F_{q^ν} of exponent μ and $\chi_{\nu,\mu}$ be the multiplicative character of F_{q^ν} induced by χ. It follows that

$$\chi_{\nu,\mu}(f_1(a)) = 1, \quad \text{for all } a \in F_{q^\nu}$$

in each case (see [18]). Moreover the number of F_{q^ν}-rational affine points of the curve Y (see for example [42] or [39]) is

$$\begin{aligned} N_{q^\nu} &= \sum_{x\in F_{q^\nu}} \prod_{i=1}^{s}(1+ \sum_{\substack{\chi \text{ : non-trivial multiplicative} \\ \text{character of exponent } \mu}} \chi_{\nu,\mu}(f(x+c_i))) \\ &= \sum_{x\in F_{q^\nu}} \prod_{i=1}^{s}\mu \\ &= \mu^s q^\nu. \end{aligned}$$

∎

3.7 Proof of Theorem 5

Note that f_1 satisfies the conditions of Lemma 4 in the respective cases. Therefore the genera of the curves g_j are as given in Table 2. By Lemma 5 it has $\mu^s q^\nu$ many F_{q^ν}-rational affine points. By normalization of the curve Y we get a non-singular model $\tilde{Y}$ without losing F_{q^ν}-rationality of these points (see for example [40], Section 5.3). Let S be the corresponding set of F_{q^ν}-rational points of $\tilde{Y}$ and $S_1 \subset S$ a subset of S. Applying Goppa's construction to

$$D_0 = \sum_{P \in S_1} P$$

and

$$D = rP_\infty$$

where $r < \deg D_0 = \mid S_1 \mid$ and P_∞ is a point of non-singular model corresponding to a point at infinity of the projectivization of the affine model Y, we get $r < n \leq \mu^s q^\nu$, $k \geq r + 1 - g$, $d \geq n - r$. Moreover if $2g - 2 < r = \deg D < n$, then $k = r + 1 - g$.

Chapter 4

Configurations of Lines and Fibre Products of Some Kummer Extensions

The purpose of this chapter is to show a correspondence between configurations of lines in $\mathbb{F}_q \times \mathbb{F}_q$ and a class of fibre products of Kummer extensions which gives families of very good codes over $\mathbb{F}_{q^2}$ improving the results of [46] and [47]. See also [37].

4.1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and X an absolutely irreducible smooth projective curve over $\mathbb{F}_q$. It is well-known that using $\mathbb{F}_q$-rational points of X we get linear codes by Goppa construction (see for example [19], [44] or [50]). For fixed q, it is important to get "good" $[n, k, d]_q$ codes, which means n is large with respect to q and $k + d$ is near to $n + 1$. Note that $n + 1 \geq k + d$ by Singleton bound.

Stepanov [46], [47] considered the curves over finite fields $\mathbb{F}_{q^2}$ of characteristic $p \neq 2$ of the form

$$y_i^2 = x + x^q + c_i \quad i = 1, 2, \ldots, s \tag{1.1}$$

where $c_1, c_2, \ldots, c_s$ are distinct elements of $\mathbb{F}_q$.

In this chapter we consider the projective curve X whose affine model is of the form

$$X: \quad y_i^{\mu_i} = \mathrm{tr}(a_i x + b_i) \quad i = 1, 2, \ldots, s$$

where $a_i \in \mathbb{F}_{q^2}^*$, $b_i \in \mathbb{F}_{q^2}$, $1 < \mu_i \mid (q+1)$ for $i = 1, 2, \ldots, s$ and $\mathrm{tr}(\alpha) = \alpha + \alpha^q$ under a condition so that the smooth projective model $\tilde{X}$ is absolutely irreducible.

We first observe a bijection between such curves and lines in $\mathbb{F}_q \times \mathbb{F}_q$.

Lemma 6 *Let $\mathbb{F}_q$ be a finite field with q elements. There is a bijection between the sets*

$$S := \{A_{a,b} \subset \mathbb{F}_{q^2} | A_{a,b} = \{\alpha \in \mathbb{F}_{q^2} | \mathrm{tr}(a\alpha + b) = 0\},\ a \in \mathbb{F}_{q^2}^*,\ b \in \mathbb{F}_{q^2}\}$$

and

$$T := \{B_{c_1,c_2,c_3} \subset \mathbb{F}_q \times \mathbb{F}_q | B_{c_1,c_2,c_3} = \{(\beta_1, \beta_2) | c_1\beta_1 + c_2\beta_2 + c_3 = 0\},\ [c_1 : c_2] \in \mathbb{P}_{\mathbb{F}_q},\ c_3 \in \mathbb{F}_q\}$$

where $\mathbb{P}^1_{\mathbb{F}_q}$ is the projective line over $\mathbb{F}_q$.

We fix the notation for S and T and fix a bijection $\phi : T \to S$. Moreover denote by $\tilde{\phi} : T \to \mathbb{F}_{q^2}[x]$ a fixed injection such that $\tilde{\phi}(B) = ax + b$ where $\phi(B) = \{\alpha \in \mathbb{F}_{q^2} | \mathrm{tr}(a\alpha + b) = 0\}$, $a \in \mathbb{F}_{q^2}^*$ and $b \in \mathbb{F}_{q^2}$.

Lemma 7 *Let $T_1 = (B_1, B_2, \ldots, B_s)$ where $B_i \in T$ such that $B_{i+1} \not\subseteq \cup_{j=1}^{i} B_j$ for $i \geq 1$. If $1 < \mu_i | (q+1)$ for $i = 1, 2, \ldots, s$, then the smooth projective curve $\tilde{X}$ whose affine model is given by*

$$X: \quad y_i^{\mu_i} = \mathrm{tr}(\tilde{\phi}(B_i)) \quad i = 1, 2, \ldots, s \tag{1.2}$$

is a Kummer extension of $\mathbb{F}_{q^2}(x)$ of degree $\prod_{i=1}^{s} \mu_i$, in particular it is absolutely irreducible.

Therefore the condition that $c_1, c_2, \ldots, c_s$ are distinct elements of $\mathbb{F}_q$ for the curve 1.1 is transformed into the condition of Lemma 7 for the curve 1.2.

To get a neat statement for our theorem we define two more functions.

Definition 1 *Let $T_1 = (B_1, B_2, \ldots, B_s)$ satisfy the condition of Lemma 7 and $1 < \mu_i | (q+1)$ for $i = 1, 2, \ldots, s$. We define the functions u_{T_1} and w_{T_1} as*

$$u_{T_1},\ w_{T_1} : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{Q}^+ \quad via$$
$$u_{T_1}(\alpha,\beta) = \frac{1}{\mu_1^{l_1(\alpha,\beta)} \cdots \mu_s^{l_s(\alpha,\beta)}}, \quad w_{T_1}(\alpha,\beta) = \frac{1}{\mathrm{lcm}(\mu_1^{l_1(\alpha,\beta)}, \ldots, \mu_s^{l_s(\alpha,\beta)})}$$

where $\alpha,\ \beta \in \mathbb{F}_q$ and

$$l_i(\alpha,\beta) = \begin{cases} 1 & \text{if } (\alpha,\beta) \in B_i \\ 0 & \text{if } (\alpha,\beta) \notin B_i \end{cases}$$

for $i = 1, 2, \ldots, s$.

Theorem 6 *Let $T_1 = (B_1, B_2, \ldots, B_s)$ satisfy the condition of Lemma 7 and $1 < \mu_i | (q+1)$ for $i = 1, 2, \ldots, s$. Then the absolutely irreducible smooth projective curve whose affine model is given by*

$$y_i^{\mu_i} = \mathrm{tr}(\tilde{\phi}(B_i)) \quad i = 1, 2, \ldots, s$$

has

$$N = 1 + (\prod_{i=1}^{s} \mu_i)(\sum_{(\alpha,\beta) \in \mathbb{F}_q \times \mathbb{F}_q} u_{T_1}(\alpha,\beta))$$

$\mathbb{F}_{q^2}$-rational affine places and has genus

$$g = 1 - \frac{1}{2}(\prod_{i=1}^{s} \mu_i)(1 + \frac{1}{\mathrm{lcm}(\mu_1, \ldots, \mu_s)}) + \frac{1}{2}(\prod_{i=1}^{s} \mu_i)(\sum_{(\alpha,\beta) \in \mathbb{F}_q \times \mathbb{F}_q} (1 - w_{T_1}(\alpha,\beta))).$$

Corollary 3 *Let $T_1 = (B_1, B_2, \ldots, B_s)$ and $T_2 = (C_1, C_2, \ldots, C_s)$ satisfy the condition of Lemma 7. Moreover assume $1 < \mu_1 = \mu_2 = \cdots = \mu_s | (q+1)$ and $\# \cup_{i=1}^{s} B_i < \# \cup_{i=1}^{s} C_i$. If X_i is the curve defined in the Theorem 6 for T_i $i = 1, 2$ respectively, then*

$$N_1 > N_2 \ \text{ and } \ g_1 < g_2$$

where N_i and g_i are the number of $\mathbb{F}_{q^2}$-rational affine points and genera for the curves X_i respectively.

Remark 5 *If $B_1, B_2, \cdots, B_s \subset \mathbb{F}_q \times \mathbb{F}_q$ are parallel affine lines and $2 = \mu_1 = \mu_2 = \cdots = \mu_s$, then the corresponding curve is the same as 1.1 that has been studied in [46] and [47]. See also Section 4.2.*

Remark 6 *Theorem 6 converts the problem into a problem of finding the "densest" configuration of lines of $\mathbb{F}_q \times \mathbb{F}_q$ in the respect of the condition of Lemma 7. This seems to be a difficult combinatorial problem. However in Section 4.2 we give two immediate examples improving the results of [46] and [47].*

Remark 7 *We improve the previous results in many respects. First of all we get much longer codes even with larger $\frac{N}{g}$ ratios, which means they are nearer to the Singleton bound. Moreover we cover all characteristics and especially the corresponding codes span a much denser spectrum. This is important since $[n, k, d]_{q^2}$ parameters are just discrete points.*

Remark 8 *The proofs are based on algebraic function field theory. One of the reasons for giving a different proof than the explicit method of Stepanov is to give a different flavour. Although this method does not compute the linear space of the regular differential forms on the curve, it is shorter. Note that since the polynomials are square-free, using the methods of [46], [47] or [36], it is possible to find explicitly the linear space of regular differential forms, i.e. to give a proof independent from the Riemann-Hurwitz genus formula.*

In Section 4.2 we apply Theorem 6 to some examples of configurations of lines in $\mathbb{F}_q \times \mathbb{F}_q$ improving the results of [46] and [47]. We prove the lemmas and Theorem 6 in Section 4.3.

4.2 Applications of Theorem 6 giving good codes

Example 1(Parallel lines). This is the configuration that Stepanov used. Namely let

$$B_i = \{(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q | \alpha + \beta + h(i) = 0\} \;\; 1 \leq i \leq q$$

where $h : \{1, 2, \ldots, q\} \to \mathbb{F}_q$ is a fixed bijection. Then $T_1 = (B_1, B_2, \ldots, B_s)$ satisfies the conditions of Lemma 7 for $s \leq q$. Assume $1 < \mu_i | (q+1)$ for $i = 1, 2, \ldots, s$, then

$$u_{T_1}(\alpha, \beta) = w_{T_1}(\alpha, \beta) = \begin{cases} \frac{1}{\mu_i} & \text{if } (\alpha, \beta) \in B_i \text{ for some } i = 1, 2, \ldots, s, \\ 1 & \text{if } (\alpha, \beta) \notin \cup_{i=1}^{s} B_i \end{cases}$$

since they are mutually disjoint. Then

$$N = (\prod_{i=1}^{s}\mu_i)(\sum_{i=1}^{s}\sum_{(\alpha,\beta)\in B_i}\frac{1}{\mu_i} + \sum_{(\alpha,\beta)\notin\cup_{i=1}^{s}B_i} 1)$$

$$= (\prod_{i=1}^{s}\mu_i)(q(\frac{1}{\mu_1}+\frac{1}{\mu_2}+\cdots+\frac{1}{\mu_s}) + (q^2-sq))$$

and

$$g = 1 - \frac{1}{2}(\prod_{i=1}^{s}\mu_i)(1+\frac{1}{\mathrm{lcm}(\mu_1,\mu_2,\ldots,\mu_s)}) + \frac{1}{2}(\prod_{i=1}^{s}\mu_i)(\sum_{i=1}^{s}\sum_{(\alpha,\beta)\in B_i}(1-\frac{1}{\mu_i}))$$

$$= 1 - \frac{1}{2}(\prod_{i=1}^{s}\mu_i)(1+\frac{1}{\mathrm{lcm}(\mu_1,\mu_2,\ldots,\mu_s)}) + \frac{1}{2}(\prod_{i=1}^{s}\mu_i)q(s-(\frac{1}{\mu_1}+\frac{1}{\mu_2}+\cdots+\frac{1}{\mu_s})).$$

In particular if $\mu = \mu_1 = \mu_2 = \cdots = \mu_s$, then

$$N = \mu^s(q\tfrac{s}{\mu} + q^2 - sq),$$

$$g = 1 - \tfrac{1}{2}\mu^s(1+\tfrac{1}{\mu}) + \tfrac{1}{2}\mu^s q(s-\tfrac{s}{\mu}).$$

Moreover if $\mu = 2$, then we get the results in [46] and [47].

Example 2(Lines through the origin). This example gives a slightly improved configuration, but Example 3 is much better. Let

$$B_i = \{(\alpha,\beta)\in\mathbb{F}_q\times\mathbb{F}q | h_1(i)\alpha + h_2(i)\beta = 0\}$$

where $h : \{1,2,\ldots,q+1\} \to \mathbb{P}^1_{\mathbb{F}_q}$ via $i \mapsto h(i) = [h_1(i) : h_2(i)]$ is a fixed bijection. Then $T_1 = (B_1, B_2, \ldots, B_s)$ satisfies the condition of Lemma 7 for $s \le q+1$. Moreover

$$u_{T_1}(\alpha,\beta) = \begin{cases} \frac{1}{\mu_i} & \text{if } (\alpha,\beta)\in B_i \text{ for some } i = 1,2,\ldots,s \text{ and } (\alpha,\beta)\neq(0,0) \\ \prod_{i=1}^{s}\frac{1}{\mu_i} & \text{if } (\alpha,\beta) = (0,0) \\ 1 & \text{if } (\alpha,\beta)\notin\cup_{i=1}^{s}B_i \end{cases}$$

and

$$w_{T_1}(\alpha,\beta) = \begin{cases} \frac{1}{\mu_i} & \text{if } (\alpha,\beta)\in B_i \text{ for some } i = 1,2,\ldots,s \text{ and } (\alpha,\beta)\neq(0,0) \\ \frac{1}{\mathrm{lcm}(\mu_1,\mu_2,\ldots\mu_s)} & \text{if } (\alpha,\beta) = (0,0) \\ 1 & \text{if } (\alpha,\beta)\notin\cup_{i=1}^{s}B_i. \end{cases}$$

Therefore

$$N = (\prod_{i=1}^{s}\mu_i)(\prod_{i=1}^{s}\frac{1}{\mu_i} + \sum_{i=1}^{s}\sum_{\substack{(\alpha,\beta)\in B_i \\ (\alpha,\beta)\neq(0,0)}}\frac{1}{\mu_i} + \sum_{(\alpha,\beta)\notin\cup_{i=1}^{s}B_i} 1)$$

$$= (\prod_{i=1}^{s}\mu_i)(\prod_{i=1}^{s}\frac{1}{\mu_i} + (q-1)(\frac{1}{\mu_1}+\cdots+\frac{1}{\mu_s}) + (q^2 - s(q-1) - 1)),$$

and

$$\begin{aligned} g &= 1 - \tfrac{1}{2}(\textstyle\prod_{i=1}^{s} \mu_i)(1 + \frac{1}{\mathrm{lcm}(\mu_1,\ldots,\mu_s)}) \\ &+ \tfrac{1}{2}(\textstyle\prod_{i=1}^{s} \mu_i)(1 - \frac{1}{\mathrm{lcm}(\mu_1,\ldots,\mu_s)} + \sum_{i=1}^{s} \sum_{\substack{(\alpha,\beta)\in B_i \\ (\alpha,\beta)\neq(0,0)}} (1 - \tfrac{1}{\mu_i})) \\ &= 1 - \tfrac{1}{2}(\textstyle\prod_{i=1}^{s} \mu_i)(1 + \frac{1}{\mathrm{lcm}(\mu_1,\ldots,\mu_s)}) \\ &+ \tfrac{1}{2}(\textstyle\prod_{i=1}^{s} \mu_i)(1 - \frac{1}{\mathrm{lcm}(\mu_1,\ldots,\mu_s)} + (q-1)s - (q-1)(\tfrac{1}{\mu_1} + \ldots + \tfrac{1}{\mu_s})). \end{aligned}$$

In particular if $\mu = \mu_1 = \mu_2 = \cdots \mu_s$, then

$$\begin{aligned} N &= \mu^s(\tfrac{1}{\mu^s} + (q-1)\tfrac{s}{\mu} + q^2 - sq + s - 1) \\ &= \mu^s((\tfrac{qs}{\mu} + q^2 - sq) + (s + \tfrac{1}{\mu^s} - \tfrac{s}{\mu} - 1)) \\ g &= 1 - \tfrac{1}{2}\mu^s(1 + \tfrac{1}{\mu}) + \tfrac{1}{2}\mu^s(1 - \tfrac{1}{\mu} + (q-1)s - (q-1)\tfrac{s}{\mu}) \\ &= 1 - \tfrac{1}{2}\mu^s(1 + \tfrac{1}{\mu}) + \tfrac{1}{2}\mu^s((qs - \tfrac{qs}{\mu}) - (s + \tfrac{1}{\mu} - \tfrac{s}{\mu} - 1)). \end{aligned}$$

Although the configuration changes slightly for $s \geq 2$, N increases and g decreases. Moreover the upper bound on s is improved from q to $q+1$ thus allowing to longer codes.

Example 3(Lines forming a net). This example is the best in these there examples. Let

$$C_i = \{(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q | \alpha + h(i) = 0\}$$

and

$$\bar{C}_i = \{(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q | \beta + h(i) = 0\}$$

where $h : \{1, 2, \ldots, q\} \to \mathbb{F}_q$ is a fixed bijection and $1 \leq i \leq q$. Let

$$B_i = \begin{cases} C_{\frac{i+1}{2}} & \text{if } i : \text{odd} \\ \bar{C}_{\frac{i}{2}} & \text{if } i : \text{even.} \end{cases}$$

Then $T_1 = (B_1, B_2, \ldots, B_s)$ satisfies the condition of Lemma 7 if $s \leq 2q - 1$. Let $s = 2s_1 < 2q$ for simplicity. Then

$$u_{T_1}(\alpha, \beta) = \begin{cases} \frac{1}{\mu_i \mu_j} & \text{if } (\alpha, \beta) \in B_i \cap B_j \text{ for some } 1 \leq i \leq j \leq s \\ \frac{1}{\mu_i} & \text{if } (\alpha, \beta) \in B_i \setminus \cup_{\substack{j=1 \\ j \neq i}}^{s} B_j \text{ for some } 1 \leq is \\ 1 & \text{if } (\alpha, \beta) \notin \cup_{i=1}^{s} B_i \end{cases}$$

and

$$w_{T_1}(\alpha,\beta) = \begin{cases} \frac{1}{\mathrm{lcm}(\mu_i,\mu_j)} & \text{if } (\alpha,\beta) \in B_i \cap B_j \text{ for some } 1 \le i \le j \le s \\ \frac{1}{\mu_i} & \text{if } (\alpha,\beta) \in B_i \setminus \cup_{\substack{j=1 \\ j\neq i}}^{s} B_j \text{ for some } 1 \le is \\ 1 & \text{if } (\alpha,\beta) \notin \cup_{i=1}^{s} B_i. \end{cases}$$

Therefore

$$\begin{aligned} N &= (\prod_{i=1}^{s})(\sum_{\substack{(\alpha,\beta)\in B_i\cap B_j \\ 1\le i\le j\le s}} \frac{1}{\mu_i\mu_j} + \sum_{\substack{(\alpha,\beta)\in B_i\setminus\cup_{\substack{j=1\\ j\neq i}}^{s} B_j \\ 1\le i\le s}} \frac{1}{\mu_i} + \sum_{(\alpha,\beta)\notin\cup_{i=1}^{s} B_i} 1) \\ &= (\prod_{i=1}^{s})((\frac{1}{\mu_1}+\frac{1}{\mu_3}+\cdots+\frac{1}{\mu_{2s_1-1}})(\frac{1}{\mu_2}+\frac{1}{\mu_4}+\cdots+\frac{1}{\mu_{2s_1}}) \\ &+(q-s_1)(\frac{1}{\mu_1}+\frac{1}{\mu_2}+\cdots+\frac{1}{\mu_{2s_1}})+q^2-(2s_1q-s_1^2)). \end{aligned}$$

and

$$\begin{aligned} g &= 1-\tfrac{1}{2}(\prod_{i=1}^{s}\mu_i)(1+\frac{1}{\mathrm{lcm}(\mu_1,\ldots,\mu_s)}) \\ &+\tfrac{1}{2}(\prod_{1}^{s}\mu_i)(\sum_{\substack{(\alpha,\beta)\in B_i\cap B_j \\ 1\le i\le j\le s}}(1-\frac{1}{\mathrm{lcm}(\mu_i,\mu_j)})+\sum_{\substack{(\alpha,\beta)\in B_i\setminus\cup_{\substack{j=1\\ j\neq i}}^{s} B_j \\ 1\le i\le s}}(1-\frac{1}{\mu_i})) \\ &= 1-\tfrac{1}{2}(\prod_{i=1}^{s}\mu_i)(1+\frac{1}{\mathrm{lcm}(\mu_1,\ldots,\mu_s)}) \\ &+\tfrac{1}{2}(\prod_{1}^{s}\mu_i)(s_1^2-\sum_{i=1}^{s_1}\sum_{j=1}^{s_1}\frac{1}{\mathrm{lcm}(\mu_{2i-1},\mu_{2j})}+(q-s_1)2s_1-(q-s_1)\sum_{i=1}^{2s_1}\frac{1}{\mu_i}). \end{aligned}$$

In particular if $\mu = \mu_1 = \mu_2 = \cdots = \mu_s$, then

$$\begin{aligned} N &= \mu^s((\tfrac{s}{2\mu})^2+(q-\tfrac{s}{2})\tfrac{s}{\mu}+q^2-(sq-\tfrac{s^2}{4})) \\ &= \mu^s((\tfrac{qs}{\mu}+q^2-sq)+(\tfrac{s^2}{4}+\tfrac{s^2}{4\mu^2}-\tfrac{s^2}{2\mu})) \\ g &= 1-\tfrac{1}{2}\mu^s(1+\tfrac{1}{\mu})+\tfrac{1}{2}\mu^s(\tfrac{s^2}{4}-\tfrac{s^2}{4\mu}+(q-\tfrac{s}{2})s-(q-\tfrac{s}{2})\tfrac{s}{\mu}) \\ &= 1-\tfrac{1}{2}\mu^s(1+\tfrac{1}{\mu})+\tfrac{1}{2}\mu^s((qs-\tfrac{qs}{\mu})-(\tfrac{s^2}{4}-\tfrac{s^2}{4\mu})). \end{aligned}$$

Therefore N increases and g decreases as s is bounded from above by $2q-1$ instead of q. This result is much better than Example 1 and Example 2.

Remark 9 *There are better configurations than Example 3. For instance lines forming a triangle is better for $s = 3$. In fact there are two problems: To increase s and for fixed s to get the "densest" configuration. These problems are*

not independent, i.e. for s_1, s_2 compatible with q, if T_1 and T_2 are configurations with s_1 and s_2 respectively such that $s_1 < s_2$, then T_1 can have larger number of rational points than T_2. Moreover if we also allow μ's to differ, the problem is more difficult.

However in any case $s < (q+1)q = |T|$ at least, so $N < \infty$ which means that these classes of curves are asymptotically bad. This also follows from the well-known result of Frey-Perret-Stichtenoth (see [8]).

4.3 Proof of Lemmas and Theorem 6

PROOF. [Proof of Lemma 6] Observe that if $a \in \mathbb{F}_{q^2}^*$ and $b \in \mathbb{F}_{q^2}$, then

$$gcd(\mathrm{tr}(x), \mathrm{tr}(ax+b)) = \begin{cases} x^q + x & \text{if } a \in \mathbb{F}_q^* \text{ and } \mathrm{tr}(b) = 0 \\ x + \frac{\mathrm{tr}(b)}{a - a^q} & \text{if } a \notin \mathbb{F}_q^* \\ 1 & \text{if } a \in \mathbb{F}_q^* \text{ and } \mathrm{tr}(b) \neq 0. \end{cases}$$

Indeed $< \mathrm{tr}(x), \mathrm{tr}(ax+b) > = < x^q + x, \mathrm{tr}(ax+b) - a^q \mathrm{tr}(x) > = < x^q + x, x(a - a^q) + \mathrm{tr}(b) >$ and if $a \notin \mathbb{F}_q^*$, then $(\frac{\mathrm{tr}(b)}{a^q - a})^q - (\frac{\mathrm{tr}(b)}{a^q - a}) = 0$.

If a, $\bar{a} \in \mathbb{F}_{q^2}^*$ and b, $\bar{b} \in \mathbb{F}_{q^2}$, then by a linear change of variables we obtain

$$gcd(\mathrm{tr}(ax+b), \mathrm{tr}(\bar{a}x+\bar{b})) = \begin{cases} \mathrm{tr}(ax+b) & \text{if } \frac{\bar{a}}{a} \in \mathbb{F}_q^* \text{ and } a\mathrm{tr}(\bar{b}) = \bar{a}\mathrm{tr}(b) \\ x + \frac{\mathrm{tr}(\bar{b} - \frac{\bar{a}}{a} b)}{\frac{\bar{a}}{a} - (\frac{\bar{a}}{a})^q} & \text{if } \frac{\bar{a}}{a} \notin \mathbb{F}_q^* \\ 1 & \text{if } \frac{\bar{a}}{a} \in \mathbb{F}_q^* \text{ and } a\mathrm{tr}(\bar{b}) \neq \bar{a}\mathrm{tr}(b). \end{cases}$$

Therefore $|S| = \frac{(q^2-1)q^2}{(q-1)q} = (q+1)q = |T|$.

Let $\{w, w^q\}$ be a fixed normal basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Moreover let $a = a_1 w + a_2 w^q$, $b = b_1 w + b_2 w^q$, $w^2 = k_1 w + k_2 w^q$, and $w^{q+1} = lw + lw^q$. Consider the map

$$\psi : S \to T$$

defined by

$$\psi(A_{a,b}) = B_{a_1(k_1+k_2)+2la_2, a_2(k_1+k_2)+2la_1, b_1+b_2}.$$

To prove the surjectivity of ψ, it is enough to prove that the matrix

$$\begin{bmatrix} k_1 + k_2 & 2l \\ 2l & k_1 + k_2 \end{bmatrix}$$

is nonsingular. Indeed it is nonsingular, otherwise $(k_1 + k_2) = \mp 2l$. Therefore $w^2 + w^{2q} = \mp w^{q+1}$ and so that $(w \pm w^q)^2 = 0$, which is a contradiction to

the fact that $\{w, w^q\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Since $|T| = |S| < \infty$, ψ is a bijection. ∎

PROOF. [Proof of Lemma 7] Let $a_1 \in \mathbb{F}_{q^2}^*$, $b_1 \in \mathbb{F}_{q^2}$ and $1 < \mu_1 | (q+1)$. Then

$$y_1^{\mu_1} = \mathrm{tr}(a_1 x + b_1)$$

is a Kummer extension of $\mathbb{F}_{q^2}(x)$. Indeed if P is a place of $\mathbb{F}_{q^2}(x)$ corresponding to a zero of $\mathrm{tr}(a_1 x + b_1)$, then $v_P(\mathrm{tr}(a_1 x + b_1)) = 1$. Therefore it is a Kummer extension of degree μ_1 (see [50] III.7.4).

Assume that $a_2 \in \mathbb{F}_{q^2}^*$, $b_1 \in \mathbb{F}_{q^2}$, $1 < \mu_1 | (q+1)$ and there exists a place Q of $\mathbb{F}_{q^2}(x)$ such that $v_Q(\mathrm{tr}(a_2 x + b_2)) = 1$ and $v_Q(\mathrm{tr}(a_1 x + b_1)) = 0$. Then by the same argument and Abhyankar's Lemma (see [50] III.8.9)

$$y_1^{\mu_1} = \mathrm{tr}(a_1 x + b_1)$$
$$y_2^{\mu_2} = \mathrm{tr}(a_2 x + b_2)$$

is a Kummer extension of degree $\mu_1 \mu_2$. By the property of T_1, for any $2 \le j \le s$ there exists a place Q_j of $\mathbb{F}_{q^2}(x)$ such that $v_{Q_j}(\tilde{\phi}(B_j)) = 1$ and $v_{Q_j}(\tilde{\phi}(B_i)) = 0$ for $i = 1, 2, \ldots, j-1$. Therefore

$$y_i^{\mu_i} = \mathrm{tr}(\tilde{\phi}(B_i)) \;\; i = 1, 2 \ldots, s$$

is a Kummer extension of $\mathbb{F}_{q^2}(x)$ of degree $\prod_{i=1}^s \mu_i$, in particular it is absolutely irreducible. ∎

PROOF. [Proof of Theorem 6] Note that if $1 < \mu | (q+1)$ and $\alpha \in \mathbb{F}_q^*$, then

$$y^\mu = \alpha$$

has μ distinct solutions in $\mathbb{F}_{q^2}$ as $\{g^{\frac{q+1}{2} t_0 + \frac{q^2-1}{\mu} s} | s = 0, 1, \ldots, \mu - 1\}$ where g is a generator of the cyclic group $\mathbb{F}_{q^2}^*$ and $\alpha = g^{(q+1)t_0}$. Therefore if $(\alpha, \beta) \notin \cup_{i=1}^s B_i$, then there exists a unique corresponding place P of $\mathbb{F}_{q^2}(x)$ such that P splits in each extension

$$y_i^{\mu_i} = \mathrm{tr}(\tilde{\phi}(B_i)) \; i = 1, 2, \ldots, s.$$

Therefore there are

$$\prod_{i=1}^s \mu_i = (\prod_{i=1}^s \mu_i) u_{T_1}(\alpha, \beta)$$

many rational places over the place P on the curve.

Similarly if $(\gamma, \delta) \in B_{i_1} \cap \ldots \cap B_{i_{s_1}}$ $1 \le s_1 \le s$, then there exists a unique corresponding place Q of $\mathbb{F}_{q^2}(x)$ such that Q splits in the extensions

$$y_i^{\mu_i} = \mathrm{tr}(\tilde{\phi}(B_i)) \;\; i \in \{1, 2, \ldots, s\} \setminus \{i_1, i_2, \ldots, i_{s_1}\}$$

and is totally ramified in the extensions

$$y_i^{\mu_i} = \mathrm{tr}(\tilde{\phi}(B_i)) \;\; i \in \{i_1, i_2, \ldots, i_{s_1}\}.$$

Therefore there are

$$\frac{\prod_{i=1}^{s} \mu_i}{\mu_{i_1}\mu_{i_2}\cdots\mu_{i_{s_1}}} = (\prod_{i=1}^{s} \mu_i) u_{T_1}(\gamma, \delta)$$

many rational places over the place Q on the curve.

Summing all these gives N the number of $\mathbb{F}_{q^2}$ rational affine points on the curve.

To prove the genus formula, first recall the Riemann-Hurwitz genus formula for tamely ramified extensions of algebraic function fields F'/F having the same constant field

$$g' = 1 + n(g-1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (e(P'|P) - 1)\deg P'$$

where $n = [F' : F]$, g' is the genus of F', g is the genus of F, $\mathbb{P}_F$ is the set of places of F and $e(P'|P)$ is the ramification index (see [50] III.5.6).

Since $F = \mathbb{F}_{q^2}(x)$, $g = 0$ and $n = \prod_{i=1}^{s} \mu_i$ by Lemma 7. Moreover $\mathrm{tr}(ax + b)$ splits over F_{q^2} for any $a \in \mathbb{F}_{q^2}^*$ and $b \in \mathbb{F}_{q^2}$. Therefore we need to take into account only the places of F corresponding to the points of $\mathbb{F}_q \times \mathbb{F}_q$ and P_∞, the place where $v_{P_\infty}(x) = -1$.

Let P_i' be a place of $F(y_i)$ over P_∞. Then $e(P_i'|P) = \mu_i$ for $i = 1, 2, \ldots, s$. If P' is a place of F' over P_∞, then by Abhyankar's Lemma (see [50] III.8.9)

$$e(P_i'|P) = \mathrm{lcm}(\mu_1, \mu_2, \ldots, \mu_s). \tag{1.3}$$

Let $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ and P be the place of F corresponding to (α, β). If P_i' is a place of $F(y_i)$ over P, then

$$e(P_i'|P) = \begin{cases} 1 & \text{if } (\alpha, \beta) \in B_i \\ 0 & \text{if } (\alpha, \beta) \notin B_i \end{cases}$$

Thus by Abhyankar's Lemma if P' is a place of F' over P, then

$$e(P'|P) = \mathrm{lcm}(\mu_1^{l_1}, \mu_2^{l_2}, \ldots, \mu_s^{l_s}) \tag{1.4}$$

where

$$l_i = \begin{cases} 1 & \text{if } P \in B_i \\ 0 & \text{if } P \notin B_i. \end{cases}$$

Therefore in particular $e(P'|P)$ does not depend on the choice of P' over P. Let $e(P) := e(P'|P)$, then

$$\begin{aligned}\sum_{P\in\mathbb{P}_F}\sum_{P'|P}(e(P'|P)-1)\deg P' &= \sum_{P\in\mathbb{P}_F}(e(P)-1)\sum_{P'|P}\deg P' \\ &= \sum_{P\in\mathbb{P}_F}(e(P)-1)\tfrac{n}{e(P)}\deg P \\ &= n\sum_{P\in\mathbb{P}_F}(1-\tfrac{1}{e(P)})\deg P\end{aligned}$$

(see the proof of [50] III.7.3.c). Therefore

$$g' = 1-(\prod_{i=1}^{s}\mu_i)+\frac{1}{2}(\prod_{i=1}^{s}\mu_i)\sum_{P\in\mathbb{P}_F}(1-\frac{1}{e(P)})\deg P.$$

Using 1.3, 1.4 and the fact that $\deg P = 1$ for places with $e(P) > 1$, we get the genus formula. This proves the theorem. ∎

Chapter 5

Towers of Function Fields over Finite Fields

For a tower $F_1 \subseteq F_2 \subseteq \cdots$ of algebraic function fields $F_i/\mathbb{F}_q$, define $\lambda := \lim_{i\to\infty} N(F_i)/g(F_i)$, where $N(F_i)$ is the number of rational places and $g(F_i)$ is the genus of $F_i/\mathbb{F}_q$. The purpose of this chapter is to calculate λ for a class of towers which was studied in [14], [15] and [53]. See also [38].

5.1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and $F/\mathbb{F}_q$ an algebraic function field, i.e. an algebraic extension of the rational function field $\mathbb{F}_q(x)$ of finite degree such that $\mathbb{F}_q$ is algebraically closed in F. We denote by $N(F)$ the number of rational places of $F/\mathbb{F}_q$ and by $g(F)$ the genus of the function field. Weil's theorem states that

$$|N(F) - (q+1)| \leq 2g(F)q^{1/2}.$$

Fixing q, for large genera g this bound could be improved. Namely let $N_q(g) = \max\{N(F)|F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g\}$ and $A(q) = \limsup_{g\to\infty} N_q(g)/g$, then by Drinfeld-Vladut bound

$$A(q) \leq \sqrt{q} - 1.$$

If q is a square, Ihara and Tsfasman-Vladut-Zink proved that

$$A(q) = \sqrt{q} - 1.$$

If q is not square, the exact value of $A(q)$ is unknown. Serre showed

$$A(q) \geq c \log q > 0 \text{ for all } q$$

with some small constant $c > 0$.

A *tower of function fields* over $\mathbb{F}_q$ is a sequence $\mathcal{F} = (F_1, F_2, \ldots)$ of function fields $F_i/\mathbb{F}_q$ having the following properties: (i) $F_1 \subsetneq F_2 \subsetneq F_3 \subsetneq \cdots$, (ii) for every $n \geq 1$, the extension F_{n+1}/F_n is separable of degree > 1, and (iii) $g(F_j) > 1$ for some $j \geq 1$. Let $\lambda(\mathcal{F}) := \lim_{n\to\infty} N(F_n)/g(F_n)$. $\mathcal{F}$ is called *asymptotically good* if $\lambda(\mathcal{F}) > 0$.

It is clear that $\lambda(\mathcal{F}) \leq A(q)$. Garcia-Stichtenoth-Thomas [14] have recently given examples for any $q = p^e$, $e \geq 2$ such that $\lambda(\mathcal{F}) \geq \frac{2}{q-2}$. Namely they constructed a tower of function fields over $\mathbb{F}_q$, $q = p^e$, where $F_n = \mathbb{F}_q(x_1, \ldots, x_n)$ and

$$x_{i+1}^m + (x_i + 1)^m = 1, \; i = 1, \ldots, n-1, \; m = \frac{p^e - 1}{p - 1}.$$

It would be interesting if the actual value of $\lambda(\mathcal{F})$ was large.

Thomas [53] showed $\lambda(\mathcal{F}) = \frac{2}{q-2}$ for a few fixed values of q.

In this chapter we prove the equality for a class of towers for any value of q when q is a square.

Theorem 7 *Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements. Let $F_n = \mathbb{F}_{q^2}(x_1, x_2, \ldots, x_n)$ be the algebraic function field where*

$$x_{i+1}^{q+1} + (x_i + 1)^{q+1} = 1, \; i = 1, 2, \ldots, n-1.$$

Let $\mathcal{F}$ be the tower of function fields over $\mathbb{F}_{q^2}$ given by $\mathcal{F} = (F_1, F_2, \ldots, F_n, \ldots)$. Then

$$\lambda(\mathcal{F}) = \frac{2}{q^2 - 2}.$$

5.2 Proof of Theorem 7

Let $\mathbb{P}_{F_n}$ denote the set of places of F_n, $n \geq 1$, P_∞ be the place of F_1 where $v_{P_\infty}(x_1) = -1$. Let

$$S(\mathcal{F}) = \{P \in \mathbb{P}_{F_1} | P \text{ is ramified in } F_n/F_1 \text{ for some } n \geq 2\}.$$

It is known that ([14], Example 2.3)

$$S(\mathcal{F}) \subseteq \{P \in \mathbb{P}_{F_1} | P \text{ is a rational place and } P \neq P_\infty\}. \tag{1.1}$$

Let

$$A_n = \sum_{P \in S(\mathcal{F})} \sum_{P' \in \mathbb{P}_{F_n}, P'|P} P'.$$

Claim: $\lim_{n\to\infty} \frac{\deg A_n}{(q+1)^n} = 0$.

The claim shows the equality of two sets in 1.1, since otherwise there would be a finite place which is unramified in all extensions and hence the limit would be positive.

By Riemann-Hurwitz genus formula

$$2g(F_n) - 2 = [F_n : F_1](2g(F_1) - 2) + \deg Diff(F_n/F_1).$$

From the claim above, more precisely from the equality of the two sets in 1.1 we have

$$\deg Diff(F_n/F_1) = [F_n : F_1]q^2 - \deg A_n$$

and therefore

$$g(F_n) = [F_n : F_1](g(F_1) - 1) + \frac{q^2[F_n : F_1]}{2} - \frac{\deg A_n}{2} + 1.$$

Moreover since P_∞ splits completely in all extensions F_n/F_1 we have $[F_n : F_1] \leq N(F_n) \leq [F_n : F_1] + \deg A_n$. Consequently our claim also proves the theorem since $[F_n : F_1] = (q+1)^{n-1}$.

Now we prove the claim. For $\alpha,\ \beta \in \mathbb{F}_q$ let $f(\alpha, \beta) = \#\{x \in \mathbb{F}_{q^2} | x^{q+1} = \alpha,\ x^{q+1} + x^q + x = -\beta\}$. Then

$$\#\{(x_1, x_2) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} | x_2^{q+1} = 1 - (x_1 + 1)^{q+1}\} = \sum_{\alpha_1 \in \mathbb{F}_q} \sum_{\beta_1 \in \mathbb{F}_q} \sum_{\beta_2 \in \mathbb{F}_q} f(\alpha_1, \beta_1) f(\beta_1, \beta_2)$$

since $x_2^{q+1} = -(x_1^{q+1} + x_1^q + x_1)$. Similarly

$$\begin{aligned}\#\{(x_1, x_2, x_3) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} | x_2^{q+1} = 1 - (x_1 + 1)^{q+1} \text{ and } x_3^{q+1} = 1 - (x_2 + 1)^{q+1}\} \\ = \textstyle\sum_{\alpha_1 \in \mathbb{F}_q} \sum_{\beta_1 \in \mathbb{F}_q} \sum_{\beta_2 \in \mathbb{F}_q} \sum_{\beta_3 \in \mathbb{F}_q} f(\alpha_1, \beta_1) f(\beta_1, \beta_2) f(\beta_2, \beta_3)\end{aligned}$$

By induction

$$\deg A_n = \sum_{\alpha \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} f^n(\alpha, \beta)$$

where $f^{i+1}(\alpha,\beta)=\sum_{h\in F_q} f^i(\alpha,h)f(h,\beta)$ $i\geq 1$.

Let $h:\{1,2,\ldots,q\}\to\mathbb{F}_q$ be a bijection such that $h(1)=1$ and $h(q)=0$. Define $G:=[G_{i,j}]_{1\leq i\leq q,1\leq j\leq q}$ where $G_{i,j}=f(h(i),h(j))$. Considering $G:\mathbb{C}^q\to\mathbb{C}^q$ and using L_1 norm we have $||G||=\max_{1\leq j\leq n}\sum_{i=1}^q|G_{i,j}|$ (see for example [4] page 165). We show $||G^3||<(q+1)^3$ which finishes the proof since $\deg A_n=\sum_{i=1}^q\sum_{j=1}^q G_{i,j}^n$.

Firstly observe that $0\leq G_{i,j}\leq 2$. The right hand side follows from the fact that if $a,\ b\in\mathbb{F}_q$ and $f(x)=gcd(x^{q+1}+a,x^{q+1}+x^q+x+b)$, then $\deg f\leq 2$. Moreover

$$\sum_{i=1}^q G_{i,j}=\begin{cases} q+1 & \text{if } j\neq 1,\\ 1 & \text{if } j=1,\end{cases} \tag{1.2}$$

since

$$\begin{aligned}\textstyle\sum_{i=1}^q G_{i,j} &= \#\{x\in\mathbb{F}_{q^2}|x^{q+1}+x^q+x=-h(j)\}\\ &= \#\{x\in\mathbb{F}_{q^2}|(x+1)^{q+1}=1-h(j)\}\\ &= \#\{x\in\mathbb{F}_{q^2}|x^{q+1}=1-h(j)\}.\end{aligned}$$

In fact $G_{i,1}=\begin{cases}1 & \text{if } i=1,\\ 0 & \text{if } i\neq 1.\end{cases}$ Similarly

$$\textstyle\sum_{j=1}^q G_{i,j}=\begin{cases} q+1 & \text{if } i\neq q,\\ 1 & \text{if } i=q,\end{cases} \quad\text{and}\quad G_{q,j}=\begin{cases}1 & \text{if } j=q,\\ 0 & \text{if } j\neq q.\end{cases} \tag{1.3}$$

Using 1.2 we get

$$\begin{aligned}\textstyle\sum_{i=1}^q G_{i,j}^2 &= \textstyle\sum_{i=1}^q\sum_{l=1}^q G_{i,l}G_{l,j}=\sum_{l=1}^q G_{l,j}\sum_{i=1}^q G_{i,l}\\ &= (q+1)\textstyle\sum_{l=1}^q G_{l,j}-qG_{1,j}\\ &= \begin{cases}(q+1)^2-qG_{1,j} & \text{if } j\neq 1,\\ 1 & \text{if } j=1.\end{cases}\end{aligned}$$

Moreover we also get

$$\begin{aligned}\textstyle\sum_{i=1}^q G_{i,j}^3 &= \textstyle\sum_{i=1}^q\sum_{l=1}^q G_{i,l}G_{l,j}^2=\sum_{l=1}^q G_{l,j}^2\sum_{i=1}^q G_{i,l}\\ &= (q+1)\textstyle\sum_{l=1}^q G_{l,j}^2-qG_{1,j}^2\\ &= \begin{cases}(q+1)^3-q(q+1)G_{1,j}-qG_{1,j}^2 & \text{if } j\neq 1,\\ 1 & \text{if } j=1.\end{cases}\end{aligned}$$

However there exists no $2\leq j\leq q$ such that $G_{1,j}^2=0$. Indeed if $G_{1,j}^2=0$, then

$$G_{1,l}G_{l,j}=0 \text{ for } l=1,\ldots,q$$

since the entries are nonnegative. Moreover the entries are bounded from above by 2 and using the properties 1.2 and 1.3, we get $G_{1,l} = 0$ for at most $\frac{q-1}{2}$ many values of l and $G_{l,j} = 0$ for at most $\frac{q-1}{2}$ many values of l. This gives a contradiction to $G_{1,j}^2 = 0$ and completes the proof.

Chapter 6

Conclusion and Remarks

The purpose of this chapter is to explain some of the themes for the possible further study and recent developments.

In this thesis we mainly deal with curves with many rational points. It is possible to write down generator matrices of various Goppa codes and to get actual parameters similar to the work of Boer for more classical curves [2]. Moreover one can apply other constructions, such as H-construction (see for example [54] page 272). The curves in this thesis give fast decoding algorithms since their construction is very simple and we know explicitly the module of regular differential forms for most of them. We have also found a nontrivial connection between a difficult finite geometry problem on configurations of affine lines in the affine plane and fibre products of Kummer extensions giving curves with many rational points. Moreover we managed to calculate an important parameter for a class of towers of function fields, which are studied recently. There are many many ways for generalizations and further work on the thesis and related areas. Now we mention just a few possibilities and recent developments.

Of course one of the main goals of the subject is to construct an asymptotically (very) "good" codes obtained from an asymptotically optimal curve over $\mathbb{F}_{q^2}$ exceeding the Gilbert-Varshamov bound (see Section 1.3). Although the existence of such sequences of curves are well-known by the celebrated paper of Tsfasman-Vladut-Zink [55] (indeed, they received the best paper award of 1983 by IEEE society), nobody could actually write down the equations of the modular curves of their paper. Manin-Vladut [27] gave a polynomial construction of these codes. They have shown that the degree of complexity for the

construction of codes from classical modular curves is of degree 20 and from Drinfeld modular curves is of degree 30. Lopez Jimenez [25] reduced the degree for Drinfeld modular curves to 17. Recently Garcia-Stichtenoth [12] [13] gave explicit towers of function fields over $\mathbb{F}_{q^2}$ $(F_i/\mathbb{F}_{q^2})_{i\geq 1}$ which are optimal. To construct corresponding Goppa codes, it is necessary to obtain explicit description of the bases for suitable vector spaces $L(D^{(i)})$ where $D^{(i)}$ is a divisor of $F_i/\mathbb{F}_{q^2}$. Voss-Hoholdt [57] could determine for F_1, F_2, and F_3. Hache [20] determined also F_4 over $\mathbb{F}_{16}$. In this direction Pellikaan-Stichtenoth-Torres [31] [32] determine explicitly Weierstrass semigroups of P_∞^i, where P_∞^i is the rational point of degree 1 corresponding naturally to the place at infinity of $F_1/\mathbb{F}_{q^2}$. However the question is still open and Ruud Pellikaan has called this process as "hunting missing functions"!

Another approach in the subject is to give an "elementary" treatment of the algebraic geometric (AG) codes. This has also been proposed as an open problem in [54]. It is desirable to give a treatment of AG codes independent of algebraic geometry, known as "AG codes without AG" [5], [6], [7], [21], and [33]. This approach is mostly impressed by Weierstrass semigroups which improve designed minimum distance of Goppa construction and is utilized in decoding of codes.

Over $\mathbb{F}_{q^2}$, curves with the maximal number of rational points, $N_{q^2} = q^2 + 1 + 2gq$, where g is the genus of the curve, are called *maximal curves*. Stöhr-Voloch [52] developed a wonderful theory of these curves improving ideas of Stepanov. Later Rainer Fuhrman, an academic child of Henning Stichtenoth, and Fernando Torres, an academic grandchild of Karl-Otto Stöhr via Arnaldo Garcia, proved that such curves may have genus only $g \leq \frac{(q-1)^2}{4}$ or $g = (q-1)q$ [9], which was conjectured by Stichtenoth-Torres [51] (see also [10]). The methods of [52] are very strong.

Recently H. Niederreiter, and C. Xing [29] improved the Serre's lower bound $A(q)$ for q not a prime using class field theory. This gives an analogous result of Tsfasman-Vladut-Zink [55] for $\mathbb{F}_{q^\nu}$ $\nu \geq 3$. However the method is not constructive.

In his thesis Michael Thomas [53] have explicitly found infinitely many distinct points in the interval $[0, q]$ which are limit points of $\frac{N_{q^2}}{g}$ ratios for various sequences of algebraic curves over $\mathbb{F}_{q^2}$. However these points form a set with only one accumulation point: 0.

Algebraic function fields (or algebraic curves) with many rational points

are also useful for cryptology [28], low-disperancy sequences [30], and fast multiplication over finite fields after an ingenious idea of Chudnovsky brothers [3], [41], [1].

REFERENCES

[1] Stéphane Ballet, "On the complexity of multiplication in certain finite extensions of finite fields", preprint.

[2] M. A. Boer, "Codes: Their Parameters and Geometry", Ph.D. Thesis, Eindhoven University of Technology, 1997.

[3] D.V. Chudnovsky, G.V. Chudnovsky, "Algebraic complexities and algebraic curves over finite fields", J. Complexity, 4, 285-316, 1988.

[4] S. N. Elaydi, "An introduction to difference equations", Springer-Verlag, New York, 1996.

[5] G.-L. Feng, and T.R.N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves", IEEE Trans. Inform. Theory, vol. 40, pp. 1003-10012, July 1994.

[6] G.-L. Feng, and T.R.N. Rao, "Improved geometric Goppa codes", Part I: Basic Theory, IEEE Trans. Inform. Theory, pp. 1678-1693, Nov. 1995.

[7] G.-L. Feng, N. Wei, T.R.N. Rao, and K.K. Tzeng, "Simplified understanding and efficient decoding of a class of algebraic-geometric codes", IEEE Trans. Inform. Theory, vol. 40, 981-1002, July 1994.

[8] G. Frey, M. Perret, H. Stichtenoth, "On the Different of Abelian Extensions of Global Fields", in Coding Theory and Algebraic Geometry Proceeding, Luminy 1991, 26-32, Lecture Notes in Mathematics, vol. 1518, Springer-Verlag, 1992.

[9] R. Fuhrman, and F. Torres, "The genus of curves over finite fields with many rational points", Manusicripta Mathematica, 89, 103-106, 1996.

[10] R. Fuhrman, A. Garcia, and F. Torres, "On maximal curves", Journal of Number theory, to appear.

[11] A. Garcia, and H. Stichtenoth, "Algebraic Function Fields over finite Fields with Many Rational Places", IEEE Transactions on Information Theory, Vol. 41, No. 6, November 1995.

[12] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound", Invent. Math., 121, p. 211-222, 1995.

[13] A. Garcia, and H. Stichtenoth, "On the asymptotic behavior of some tower of function fields over finite fields", Journal of Number Theory, to appear.

[14] A. Garcia, and Stichtenoth H., "Asymptotically good towers of function fields over finite fields", C.R. Acad. Sci. Paris 322, Ser. I, pp. 1067-1070, 1996.

[15] A. Garcia, H. Stichtenoth, and M. Thomas, "On towers and composite of towers of function fields over finite fields", Finite Fields and Their App., vol. 3, no. 3, pp. 257-274, 1997.

[16] G. van der Geer and M. van der Vlugt, "Fiber products of Artin-Schreier curves and generalized Hamming weights of codes", J. Comb. Theory A, 1995, 70, no. 2, p. 337-348.

[17] M. Glukhov, "Lower bounds for character sums over finite fields", Diskrt. Math., 1994, 6, no. 3, 136-142 (in Russian).

[18] M. Glukhov, "On lower bounds for character sums over finite fields", preprint.

[19] V.G. Goppa, "Codes on algebraic curves", Soviet Math. Dokl., 1981, 24, 170-172.

[20] G. Hache, "Construction effective des code géomértiques, Thése, Paris VII, 1996.

[21] T. Hoholdt, J.V. van Lint, and R. Pellikaan, "Algebraic geometric codes", preprint.

[22] Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields", J. Fac. Sci. Tokyo, 28, 721-724, 1981.

[23] S. Lang, "Algebra", Third Edition, Addison-Wesley, June 1994.

[24] R. Lidl, and H. Niederreiter, "Finite Fields", Encyclopedia of Mathematics and Its Applications, Vol. 20, Second Edition, Cambridge Univ. Press, Cambridge, U.K., 1997.

[25] B. Lopez Jimenez, "Plane models of Drinfeld modular curves", Ph.D. Thesis, Univ. Complutense, Madrid, March 1996.

[26] Y. I. Manin, "What is the maximum number of points on a curve over F_2?", J. Fac. Sci. Univ. Tokyo 28, 715-720, 1981.

[27] Y. I. Manin, and S. Vladut, "Linear Codes and Modular Curves", Journ. Sov. Math., vol. 30, pp. 2611-2643, 1985.

[28] V. Müller, "Fast Multiplication on Elliptic curves over small fields of characteristic two", preprint.

[29] H. Niederreieter, and C. Xing, "Towers of global function fields with asymptotically many rational places", preprint.

[30] H. Niederreieter, and C. Xing, "Low-Disperancy sequences and global function fields with many rational places", Finite Fields and Their Applications, 2, 241-273, 1996.

[31] R. Pellikaan, "Asymptotically good sequences of curves and codes", Proceeding Allerton Conference, University of Illinois, Urbana-Champaign, October 1996.

[32] R. Pellikaan, H. Stichtenoth, and F. Torres, "Weierstrass Semigroups in an Asymptotically good tower of function fields", preprint.

[33] R. Pellikaan, "On the existence of order functions", in Proceeding second Shangai Conference on Designs, Codes and Finite Geometry, 1996.

[34] F. Özbudak, "On lower bounds for incomplete character sums over finite fields", Finite Fields and Their Applications, 2, 173-191, 1996.

[35] F. Özbudak, and M. Glukhov, "Codes on Superelliptic Curves", preprint.

[36] F. Özbudak, "Codes on Fibre Products of Some Kummer Coverings", preprint.

[37] F. Özbudak, "On Configurations of Lines in $\mathbb{F}_q \times \mathbb{F}_q$ and Fibre Products of Some Kummer Coverings", preprint.

[38] F. Özbudak, and M. Thomas, "A Note on Towers of Function Fields over Finite Fields", preprint.

[39] W. Schmidt, "Equations over Finite Fields-An Elementary Approach", Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, 1976.

[40] I.R. Shafarevich, "Basic Algebraic geometry 1", second edition, Springer-Verlag, Berlin, 1994.

[41] I.E. Sharplinsky, M.A. Tsfasman, and S.G. Vladut, "Curves with many points and multiplication in finite fields", Lecture otes in Mathematics, 1518, 145-169, Springer-Verlag, Belin, 1992.

[42] S.A. Stepanov, "On lower bounds of sums of characters over finite fields", Discrete Math. Appl., 1992, Vol. 2, no. 5, 523-532.

[43] S.A. Stepanov, "On lower estimates of incomplete character sums of polynomials", Proceedings of the Steklov Institute of Mathematics, A.M.S., 1980 Issue 1, 187-189.

[44] S.A. Stepanov, "Error Correcting Codes and Algebraic Curves", to be published.

[45] S.A. Stepanov, "Arithmetic of Algebraic Curves", Plenum, New York, 1994.

[46] S.A. Stepanov, "Character Sums and Coding Theory", Finite Fields and Their Application, edited by S. Cohen and H. Niederreiter, pp. 355-378, Cambridge University Press, 1996.

[47] S.A. Stepanov, "Codes on fibre products of hyperelliptic curves", Discrete Math. Appl., vol. 7, no. 1, pp. 77-88, 1997.

[48] S.A. Stepanov and F. Özbudak, "Fibre products of hyperelliptic curves and geometric Goppa codes", Discrete Math. Appl., vol. 7, no. 3, pp. 223-229, 1997, to appear.

[49] S.A. Stepanov, and F. Özbudak, "Fibre Products of Superelliptic Curves and Codes Therefrom", Proceedings 1997, IEEE International Symposium on Information Theory, Ulm-Germany, pp. 413.

[50] H. Stichtenoth, "Algebraic Function Fields", Springer-Verlag, Berlin, 1993.

[51] H. Stichtenoth, and C. Xing, "The genus of maximal function fields", Manusicipta Mathematica, 86, 217-224, 1995.

[52] K.O. Stöhr, and F. Voloch, "Weierstrass points and curves over finite fields",Proc. London Math. Soc., (3), 52, pp. 1-19, 1986.

[53] M. Thomas, "Türme und Pyramiden algebraischer Funktionenkörper", Ph.D. Dissertation, University of Essen, 1997.

[54] M.A. Tsfasman, and S.G. Vladut, "Algebraic-Geometric Codes", Kluwer Academic Publishers, Dordrecht/Boston/London, 1991.

[55] Tsfasman M.A., Vladut S.G., Zink T., "Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound", Math. Nach., 109, 21-28, 1982

[56] C. Xing, "Multiple Kummer extensions and the number of prime divisors of degree one in function fields", J. of Pure and Appl. Algebra, 1993, 84, p. 85-93.

[57] C. Voss, T. Hoholdt, "An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zinl bound. The first steps", IEEE Trans. Inform. Theory, 43, 120-135, 1997.

[58] A. Weil, "Number of solutions of equations in finite fields", Bull. of the American Math. Soc., 55 (1949), 497-508.

Vita

Ferruh Özbudak was born in Gelibolu, on December 8, 1970. He received his B.S. degree from the Electrical and Electronics Engineering Department, Bilkent University in June 1993. After then, he continued his studies in the Department of Mathematics, Bilkent University as a graduate assistant. He got his M.S. degree in June 1995 under the supervision of Prof. Dr. S. A. Stepanov by the thesis entitled "On Lower Bounds of Character Sums over Finite Fields". In 1997 he visited Prof. Dr. H. Stichtenoth at Universität Essen, Germany. His research interests include algebraic curves, algebraic function fields, number theory and coding theory. After September 1997, he will return to Universität Essen.